Contenidos del CD

Suites de seguridad

AVG Internet Security 8.5
Esta suite te ofrece antivirus, antispyware, antirootkit, filtro antispam, protección contra sitios web maliciosos y protección firewall, entre otras protecciones.

BitDefender Total Sec. 2010
Paquete de seguridad con funciones de mantenimiento y mejora del rendimiento global del equipo ante posibles amenazas dañinas.

FortiClient Endpoint Prot. 4.1
Aplicación gratuita que cuenta con un potente cortafuegos a prueba de intrusos. De este modo, se garantiza la fiabilidad de la información.

G Data TotalCare 2010
Esta aplicación incorpora nuevas tecnologías como el fingerprinting y las listas blancas inteligentes para mejorar su eficacia.

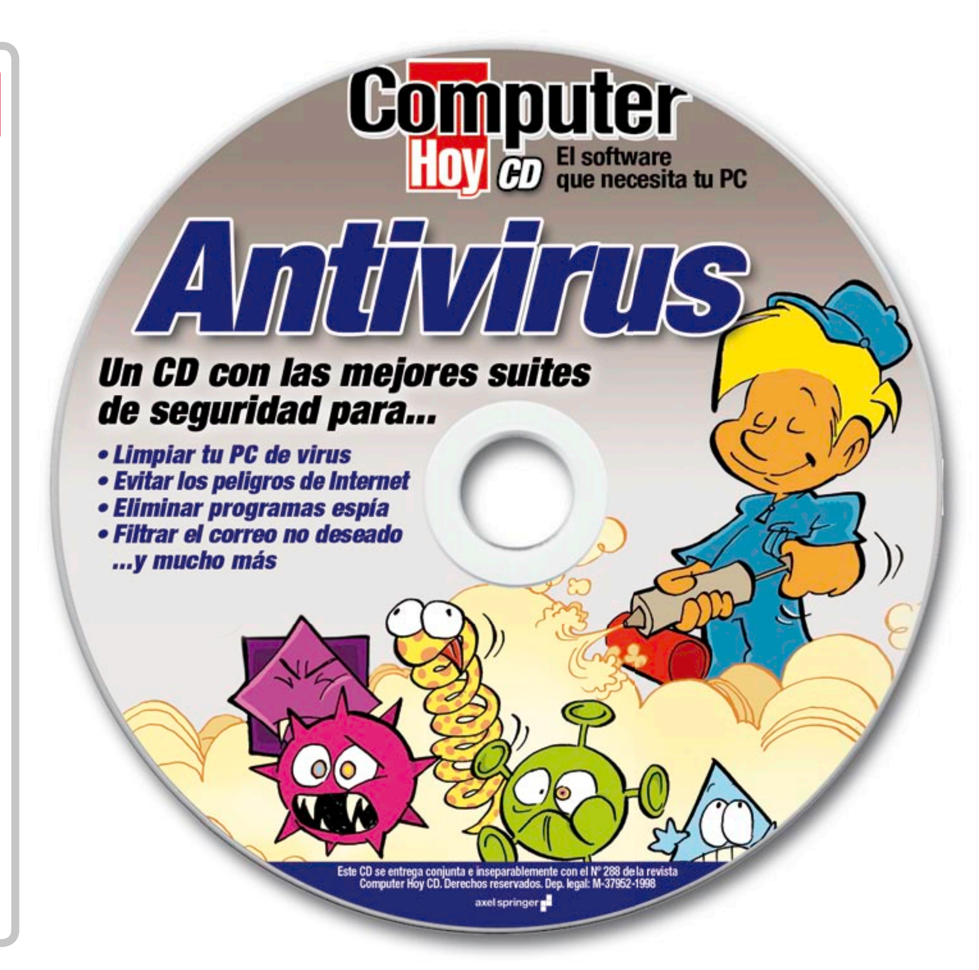
Kaspersky Internet S. 2010
Esta suite ofrece una protección total para tu PC, garantizando las compras online y la identificación de los datos del usuario.

McAfee Total Protec. 2010
Esta aplicación proporciona seguridad integral gracias a la tecnología Active Protection. De esta forma, se localiza la amenaza potencial antes de que comience su dañino efecto sobre el PC.

Norton 360 v3
Incluye funciones como antivirus, cortafuegos, copias de seguridad y optimización de disco, todas ellas con el objetivo común de aportar la mejor defensa posible contra cualquier tipo de malware.

Panda Global Protec. 2010
Potente herramienta de seguridad que integra un motor antispam y control parental. Además, el soporte de actualización proporcionado por Panda Labs asegura una base de datos siempre al día.

Trend Micro I. S. Pro 2010
Esta aplicación te defiende de spyware y estafas, mientras que un analizador de amenazas verifica que no haya virus ya erradicados del PC con anterioridad. Incluye también herramientas de utilidad para optimizar el equipo.



Para cualquier duda envíanos un email a: computerhoy@axelspringer.es

Protege tu ordenador al completo durante más de un año

Sumario

Hay software que, por su importancia, no debería faltar nunca en ningún ordenador. En esta categoría entran las aplicaciones de productividad, las de optimización del equipo, las de comunicaciones y, por supuesto, las de seguridad.

Tener el ordenador a salvo de virus, troyanos, spyware y todo tipo de malware en general resulta imprescindible para el buen funcionamiento del ordenador y, además, evita la pérdida de datos importantes.

Por este motivo, en este número de Computer Hoy te ofrecemos la posibilidad de evaluar las últimas versiones de siete suites de seguridad, lo que le aportará, en total, más de un año de protección a tu PC.

Una por una

La gran ventaja de estas aplicaciones es que, desde una consola común, es posible gestionar todas y cada una de las funciones importantes de seguridad de tu sistema.

Así, por ejemplo, podrás realizar un chequeo de tu disco duro en busca de virus o cualquier otro programa malicioso, establecer un filtro antispam para bloquear todos los correos basura que te lleguen al buzón, configurar el firewall y establecer prioridades para determinadas aplicaciones, o evitar los programas espía.



Además, todas estas suites de seguridad te ayudan a proteger tu ordenador mientras navegas por Internet. En general, evitan que te timen identificando las páginas web seguras, te ayudan a realizar compras online sin problemas y bloquean cualquier intento por parte de determinados sitios web de conocer tus patrones de navegación.

Como complemento, algunas de estas aplicaciones incluyen funciones interesantes como la protección de datos privados o el control parental, que ayuda a los padres a proteger a sus hijos del contenido de determinadas páginas web mientras navegan por Internet.

Desinstalar antes de cargar

Ahora bien, si decides instalar varios de estos programas de seguridad para probarlos, ten en cuenta no cargar ninguno sin antes desinstalar otro. Para que todo funcione correctamente y no tengas ningún problema de compatibilidad, en un PC sólo puede estar instalado un único programa de seguridad.

Instalación

Lo primero que debes hacer es introducir el CD en tu ordenador para comenzar a cargar los ficheros. Una vez seleccionada la suite que quieres, pulsa en Instalar y, en la ventana emergente que te aparezca, haz click sobre Abrir. En pocos segundos podrás empezar a disfrutar de ella.

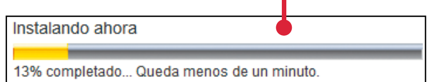


Haz frente a virus, spyware, phishing y todo tipo de código malicioso con la versión 3 del software Norton 360, de Symantec. Esta completa suite de seguridad te permite detectar posibles infecciones, reparar el equipo en caso de intrusiones y realizar copias de seguridad para restaurarlas si algún malware ha ocasionado daños en el PC. Y todo ello, desde una sencilla interfaz en castellano. Puedes saber más desde la web www.symantec.com/es

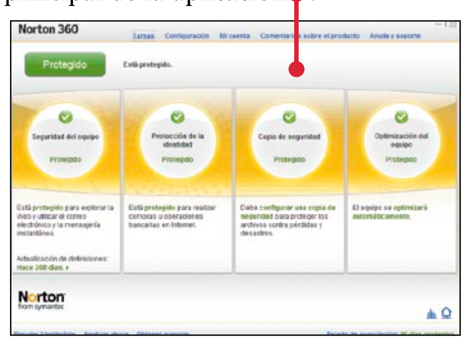
Protección total

Reparar amenazas y riesgos de seguridad, proteger la identidad del usuario, realizar backups y optimizar el funcionamiento del ordenador: ésas son las cuatro funciones principales de Norton 360 v3. Utiliza la versión gratuita incluida en el CD, válida durante 90 días, y podrás sacarle el máximo partido a estas opciones para tener tu equipo siempre a punto.

1 Cuando comiences la instalación de Norton 360 aparecerá un acuerdo de licencia que debes aceptar. Para ello, presiona en el botón ACEPTAR E INSTALAR y el proceso se pondrá en marcha, lo que puede llevarte varios minutos.



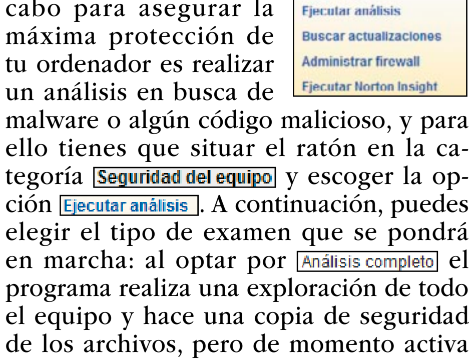
Una vez que finalice, el programa se iniciará automáticamente y su icono se agregará a la barra de tareas de tu escritorio. Si haces doble click sobre dicho símbolo, podrás ver la pantalla principal de la aplicación.



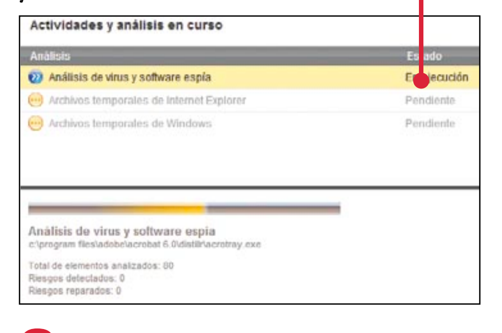
Además, su interfaz indica el estado de seguridad en el que se encuentra tu PC Protegido, para que sepas si es necesario realizar algún tipo de análisis.

2 Como puedes comprobar, Norton 360 incluye cuatro categorías principales de protección para tu equipo.

Cuando sitúes el ratón sobre cualquiera de las alternativas, el contenido mostrado cambiará para que puedas ver todas las funciones asociadas.



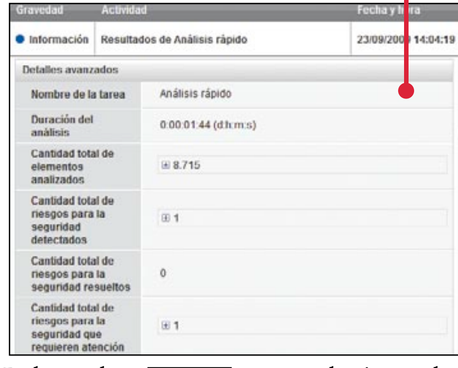
Una de las primeras tareas que debes llevar a cabo para asegurar la máxima protección de tu ordenador es realizar un análisis en busca de malware o algún código malicioso, y para ello tienes que situar el ratón en la categoría Seguridad del equipo y escoger la opción Ejecutar análisis. A continuación, puedes elegir el tipo de examen que se pondrá en marcha: al optar por Análisis completo el programa realiza una exploración de todo el equipo y hace una copia de seguridad de los archivos, pero de momento activa la casilla Análisis rápido (recomendado) para un examen instantáneo. Presiona en el botón Ir y comenzará a realizarse el análisis.



3 Pueden pasar unos cuantos minutos hasta que Norton 360 finalice la búsqueda y, una vez que termine, se mostrarán todos los elementos sospechosos que requieren algún tipo de atención.

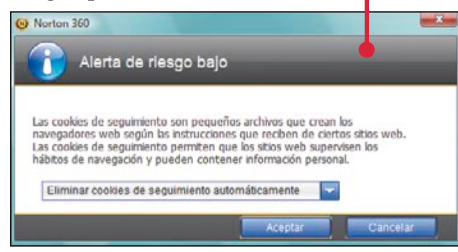


Si, además, presionas en Detalles, verás los datos del análisis con más profundidad y los elementos que han sido examinados.

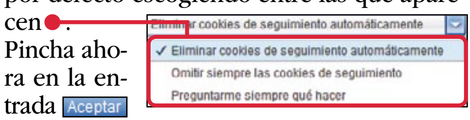


Pulsa sobre Reparar para solucionar los posibles problemas detectados, de modo que una nueva pantalla te mostrará en qué consiste el riesgo.

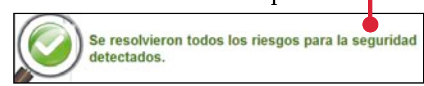
Aunque el programa te ofrece una acción por defecto, pulsando en la flecha puedes desplegar todas las operaciones posibles. Mantén la que aparece en la aplicación y presiona en el botón Aceptar. Es posible que una nueva pantalla te indique el nivel de riesgo que tiene dicha amenaza



y de nuevo podrás elegir qué opción utilizar por defecto escogiendo entre las que aparecen.

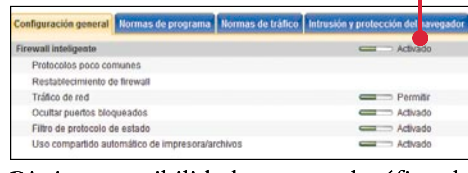


Pincha ahora en la entrada Aceptar y Norton 360 reparará la amenaza, tal como te indica un aviso en pantalla.

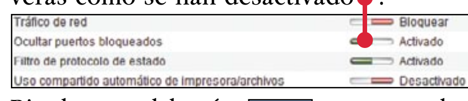


Por último, presiona en Finalizar.

4 Otra de las tareas que puedes llevar a cabo desde la función Seguridad del equipo es la de gestionar el cortafuegos del programa, así que coloca el ratón sobre ella y escoge Administrar firewall. Ten en cuenta que, al instalar el antivirus, automáticamente se deshabilitará el cortafuegos de Windows y se activará el de Norton 360, como puedes ver en la nueva ventana que aparece.



Distintas posibilidades como el tráfico de red o el uso compartido de recursos se encuentran también habilitadas, aunque si deseas bloquear alguna de ellas solamente tienes que pulsar sobre la opción Activado o bien sobre Permitir, y verás cómo se han desactivado.



Pincha en el botón Aplicar para que los cambios se hagan efectivos.

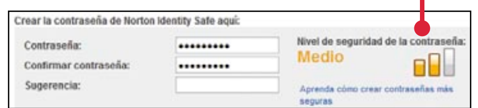
5 A continuación, puedes determinar si el firewall bloqueará el acceso a alguna aplicación, así que acude a la pestaña Normas de programa. Asociado a cada aplicación aparece el tipo de acceso permitido.



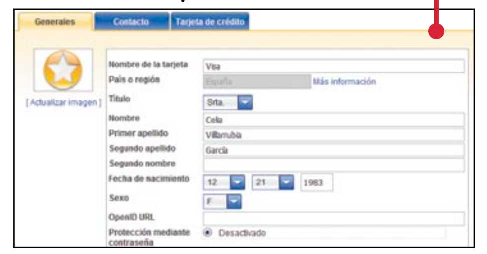
aunque tú podrás modificar cada categoría en función de tus intereses, escogiendo entre alguna de las opciones ●.



Si quieres añadir algún programa al listado para aceptar el acceso desde tu ordenador, haz click en el botón Agregar, selecciona en tu PC esa aplicación en concreto DeskTube.exe y, cuando Norton 360 te pregunte qué deseas hacer con el acceso, selecciona la opción Permitir y presiona en Aceptar. De este modo, el nuevo programa aparecerá en el listado ●.



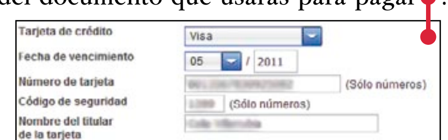
6 Por otra parte, Norton 360 cuenta también con una función de protección de la identidad para realizar compras u operaciones bancarias por Internet con seguridad, denominada Identity Safe. Para configurar esta alternativa, debes situar el ratón sobre la opción ● Protección de la identidad y elegir Configurar Identity Safe, de modo que se despliegue una nueva ventana, en la que debes escribir una contraseña que te será solicitada en el momento de acceder a Internet ●.



Presiona a continuación sobre el botón Siguiente. En la pantalla que aparece puedes escribir información personal sobre ti, como tu nombre y fecha de nacimiento ●.



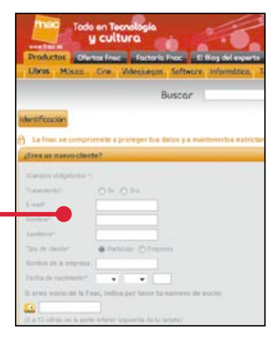
Si pinchas en la pestaña Contacto podrás indicar los datos necesarios para poder localizarte, como tu teléfono o tu dirección ●



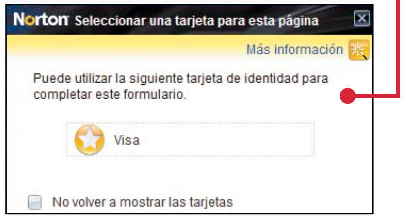
y desde Tarjeta de crédito introduce los detalles del documento que usarás para pagar ●.

Por último, pincha en Guardar.

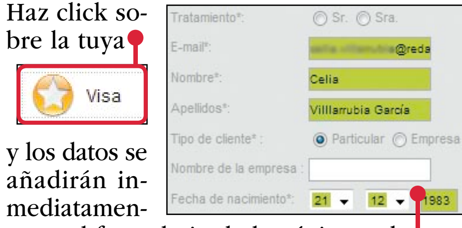
7 Una vez que tus datos estén almacenados, es posible que se muestren automáticamente a la hora de realizar una compra de forma online. Por ejemplo, inicia el proceso de adquisición en una tienda virtual ●



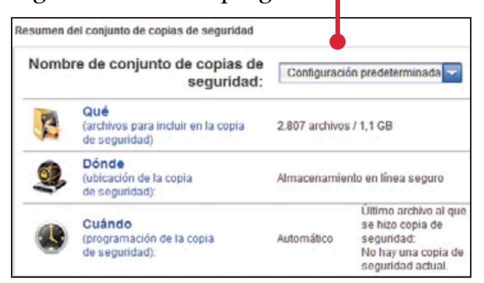
y, cuando tengas que introducir la información de tu perfil, una ventana emergente te mostrará las tarjetas de identidad que has creado previamente ●.



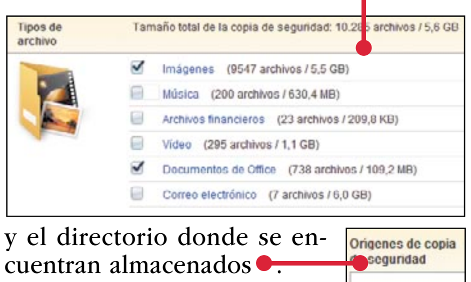
Haz click sobre la tuya ● Visa y los datos se añadirán inmediatamente en el formulario de la página web ● para que el proceso de compra sea más sencillo y mucho más seguro.



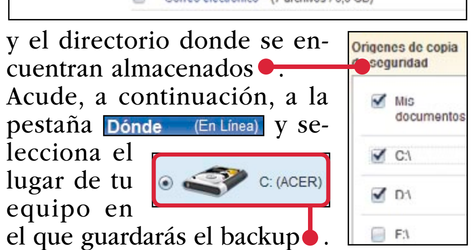
8 No olvides echarle también un vistazo a la función Copia de seguridad, para poder realizar backups del contenido de tu ordenador. Pulsa sobre la entrada ● Ejecutar copia de seguridad ahora y verás el tamaño que tendrá la copia de seguridad y el lugar donde se almacenará, según establece el programa ●.



Para modificar estos parámetros pulsa primero en Qué (6,2 GB) y escoge los tipos de archivo que quieres guardar ●

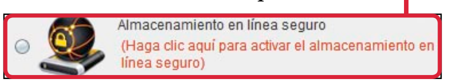


y el directorio donde se encuentran almacenados ●.

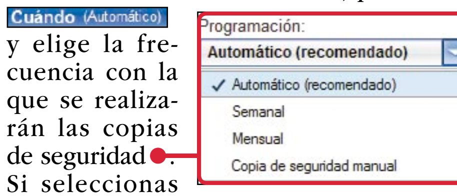


Acude, a continuación, a la pestaña Dónde (En Línea) y selecciona el lugar de tu equipo en el que guardarás el backup ●.

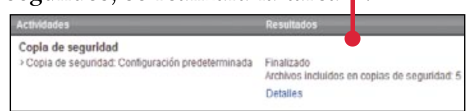
Ten en cuenta que puedes optar por el almacenamiento online pulsando en ●



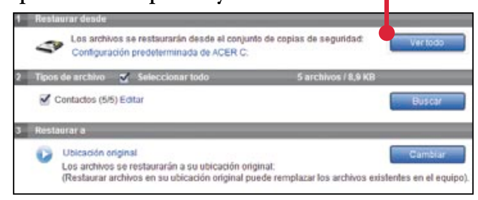
aunque para eso deberás registrarte primero en Norton 360. Por último, pincha en Cuándo (Automático) y elige la frecuencia con la que se realizarán las copias de seguridad ●.



Si seleccionas Copia de seguridad manual, el programa sólo llevará a cabo un backup cuando lo solicites, para lo que deberás hacer click en el botón Ejecutar copia de seguridad y, en unos pocos segundos, se realizará la tarea ●.

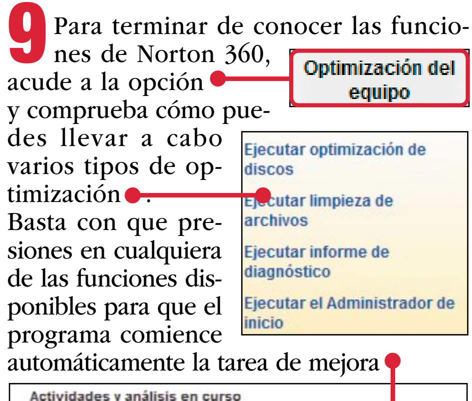


Posteriormente, podrás restaurar alguna de las copias realizadas pulsando sobre Restaurar archivos y eligiendo, en la ventana que aparece a continuación, el archivo que quieres recuperar y su ubicación ●.

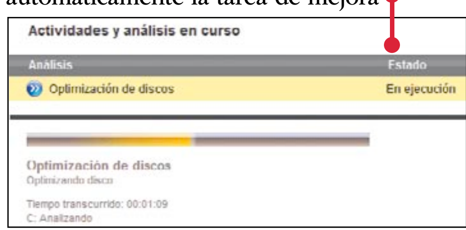


Presiona luego en Restaurar archivos y recuperarás tus copias de seguridad.

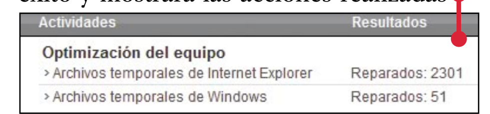
9 Para terminar de conocer las funciones de Norton 360, acude a la opción ● Optimización del equipo y comprueba cómo puedes llevar a cabo varios tipos de optimización ●.



Basta con que presiones en cualquiera de las funciones disponibles para que el programa comience automáticamente la tarea de mejora ●



que puede alargarse durante varios minutos. Una vez que finalice, la aplicación te indicará que la tarea se ha realizado con éxito y mostrará las acciones realizadas ●



de modo que podrás pasar a optimizar otra de las áreas posibles. Así tendrás siempre a punto tu equipo para trabajar con él sin problemas y sin riesgos de seguridad.

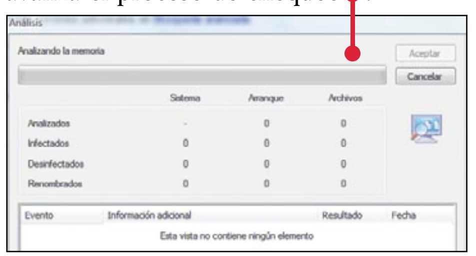


Cuanto mayor sea el área de actuación de una suite de seguridad informática, más a salvo estará nuestro equipo. Así lo entienden los desarrolladores de Panda Global Protection 2010, y buena prueba de ello es que este entorno comprende herramientas antivirus, tecnología TruePrevent, antispyware, firewall y backup, entre otras utilidades. Si deseas conocer más detalle sobre su utilización, no dudes en visitar su página web www.pandasecurity.com

Garantiza la seguridad completa de tu PC

Lamentablemente, las amenazas de malware evolucionan cada día para resultar aún más dañinas. Por este motivo, la única manera de conservar la integridad de los sistemas pasa por disponer de un entorno de seguridad fiable, potente y continuamente actualizado. Éste es el perfil que cumple a la perfección Panda Global Protección 2010, un conjunto de aplicaciones que aporta una de las mejores barreras para frenar toda clase de virus, spam y troyanos.

1 Poco después de comenzar su instalación, Panda Global Protection 2010 realiza un análisis completo de todo el sistema. El sentido de esta operación no es otro que el de limpiar cualquier virus residente en memoria, antes de que la suite empiece a supervisar el flujo de datos entrantes y salientes del ordenador. Para ello, aparece una nueva ventana emergente que muestra, en primer lugar, una barra horizontal que rellena su contenido según avanza el proceso de chequeo.

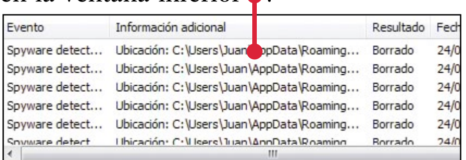


2 Durante esta primera prueba se revisan todas las áreas de la memoria del PC, aunque la aplicación las diferencia por las categorías.

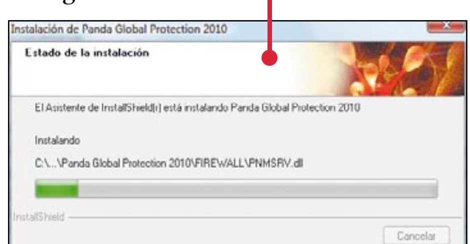
Sistema Arranque Archivos

De este modo, una que vez finaliza el análisis en busca de malware, aquellas zonas en donde se ha encontrado algún tipo de amenaza cambian su título para mostrarse en rojo Sistema. Después, en cada una de las tres columnas se detalla cuántos archivos se han catalogado como infectados, cuántos han podido ser recuperados y cuáles han cambiado su nombre.

3 En el caso de que compruebes que la herramienta ha encontrado algunos archivos dañinos que no han sido desinfectados, no te preocupes. En muchos casos los virus se introducen en el ordenador mediante un fichero añadido a la memoria, totalmente prescindible para el buen funcionamiento del equipo. De ser así, Panda Global Protection 2010 borra directamente el archivo para neutralizar la amenaza, aunque siempre se puede ver su ubicación hasta la fecha de eliminación en la ventana inferior.



Para concluir esta primera revisión, pulsa el botón Aceptar. Al instante, el programa continuará su instalación grabando el resto de registros necesarios.

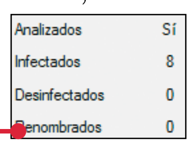


4 Una de las ventajas que aporta este conjunto de herramientas de seguridad es el control de amenazas desde los propios laboratorios del fabricante. No obstante, esta utilidad opcional es necesario activarla, marcando la correspondiente casilla verificable en la pantalla del asistente de instalación.



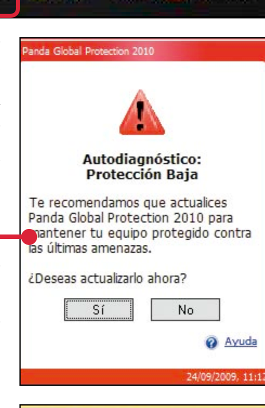
Igualmente, desde el mismo apartado también se puede aceptar el envío online de documentos en cuarentena, para que Panda Labs pueda generar cuanto antes la vacuna más precisa.

5 Panda Global Protection 2010 entra en funcionamiento desde el primer instante en el que el ordenador empieza a ejecutarse. Por ello es recomendable que, al término de la instalación o, lo que es lo mismo, cuando aparezca la pantalla, selecciones la línea con el siguiente texto Sí, deseo reiniciar el equipo ahora. y, seguidamente, pulses el botón Finalizar.



Analizados	Sí
Infectados	8
Desinfectados	0
Renombrados	0

6 Habitualmente, cuando el sistema operativo termine de cargar su registro, podrás comprobar el modo activo de este programa de seguridad mediante la aparición de su icono en la barra de herramientas de Windows. Además, en el caso de detectar que sus contenidos no están actualizados, automáticamente el programa mostrará la pantalla de enlace online. En la versión incluida en el CD, podrás disponer durante 60 días de todas las actualizaciones necesarias que el desarrollador vaya incluyendo en su web, tal y como recuerda la ventana informativa.



7 Para empezar a utilizar las utilidades de esta aplicación, haz doble click sobre su icono en la barra de herramientas de Windows. Acto seguido, podrás observar cómo aparece la que es su interfaz principal.



Antes de nada, recuerda que si en el encabezado se refleja el siguiente estado Peligro debes actualizar los datos del programa. Para ello, pulsa sobre el botón con el texto Solucionar y sigue las instrucciones del asistente de configuración que se abre a continuación. Como pronto descu-

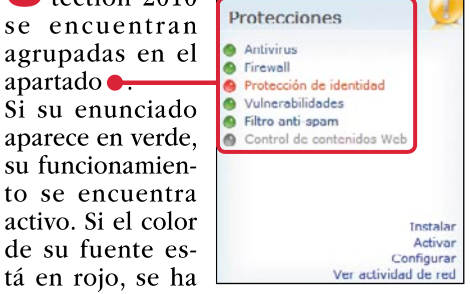


brirás, este proceso tan solo requiere unos pocos pasos .



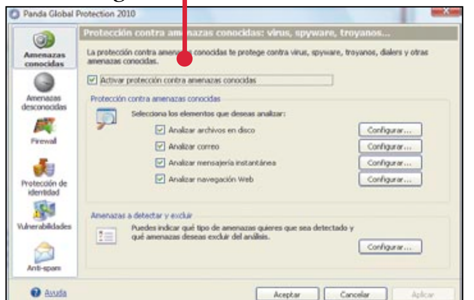
A su término, el encabezado mostrará su nuevo estado en color verde.

8 Las utilidades de Panda Global Protection 2010 se encuentran agrupadas en el apartado .



Si su enunciado aparece en verde, su funcionamiento se encuentra activo. Si el color de su fuente está en rojo, se ha anulado temporalmente su utilización. Por último, si su texto se muestra en gris quiere decir que la herramienta todavía no ha sido configurada. Para elegir cualquiera de estas aplicaciones, haz click sobre su línea correspondiente.

9 Por ejemplo, si optas por definir la función Antivirus, tras seleccionarla con el cursor aparece en la pantalla la ventana emergente .



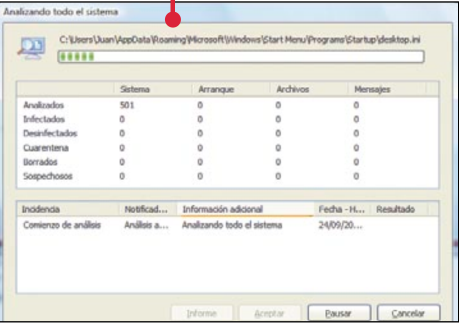
En realidad, desde esta pantalla intermedia también se puede acceder directamente a los diferentes apartados de configuración ya que, de igual modo, al pulsar cualquiera de las herramientas del menú principal se muestran las mismas utilidades listadas en la columna .

10 Después, para ordenar un análisis a la búsqueda y eliminación de códigos maliciosos, en la pantalla principal haz click sobre la pestaña Analizar. Como ahora puedes contemplar, en su interior se listan hasta cinco categorías distintas para evaluar eficazmente la seguridad del equipo .

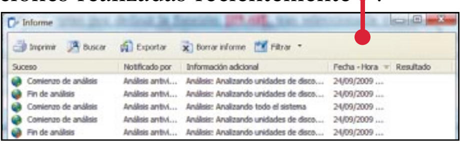
11 Prueba ahora a realizar una revisión global pulsando sobre la siguiente sentencia:



Como resultado de esta operación, el programa inicia la exploración de la memoria contrastando los documentos encontrados con su extensa base de datos sobre malware .



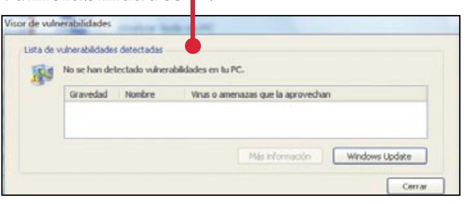
Luego, en cuanto finaliza este proceso, una frase resume de forma sencilla la cantidad de amenazas detectadas ¡No se han encontrado virus, ni otro software malicioso!. Además, en el caso de querer ampliar la información resultante, se puede escoger la entrada Informe para que, justo después, se aporte un extracto de todas las operaciones realizadas recientemente .



12 Por otro lado, si quieres averiguar si tu cuenta de correo favorita ha sido blanco de algún ataque dañino, escoge dentro de la pestaña Analizar la entrada .

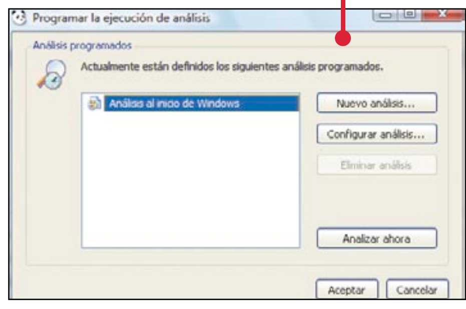


De igual modo, puede que lo que te interese sea examinar los ajustes del sistema para descubrir algún punto débil. Si éste es el caso, haz click sobre la entrada . Al instante, un explorador revisará los parámetros establecidos hasta ofrecer un resultado con todas las posibles vulnerabilidades .

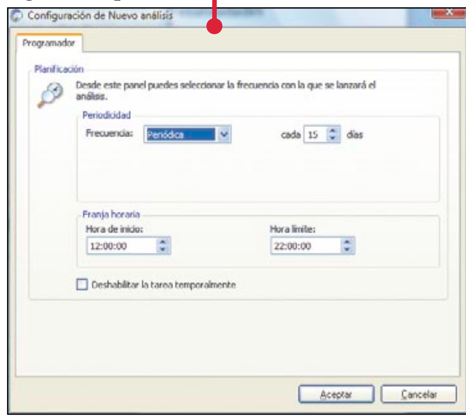


13 Defender el PC ante los virus de todo tipo no debería ser una tarea puntual, sino más bien una rutina repetida de forma periódica. Si deseas, de este modo, establecer unos ciclos fijos de revisión, pulsa el vínculo Programar la ejecución de análisis dentro de la pantalla Analizar. Este enlace abre a continuación un asistente de configuración que incluye por defecto una ejecución de análisis al inicio de Windows .





No obstante, si deseas añadir otras variantes, tan solo es necesario seleccionar la función Nuevo análisis... . Hecho esto, y tras validar algunas pantallas intermedias que establecen el área que hay que examinar de forma repetida, puedes concretar el intervalo temporal mediante los menús de la siguiente pantalla .

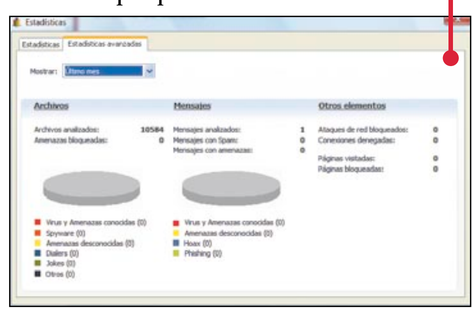


Finalmente, para que entre en funcionamiento presiona el botón Aceptar.

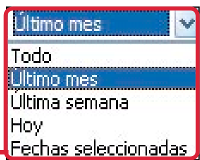
14 Por último, con el tiempo y el uso habitual de esta aplicación descubrirás su práctica eficiencia. Además, siempre que desees evaluar cómo han resultado los análisis efectuados, nada mejor que acudir a la pestaña Informe y, más concretamente, a la entrada .

Ver estadísticas

Tras ser seleccionada, un gráfico por sectores muestra las detecciones de las diferentes categorías de malware que puedan existir en el disco



con la posibilidad adicional de establecer el intervalo temporal tenido en cuenta mediante la pestaña desplegable .



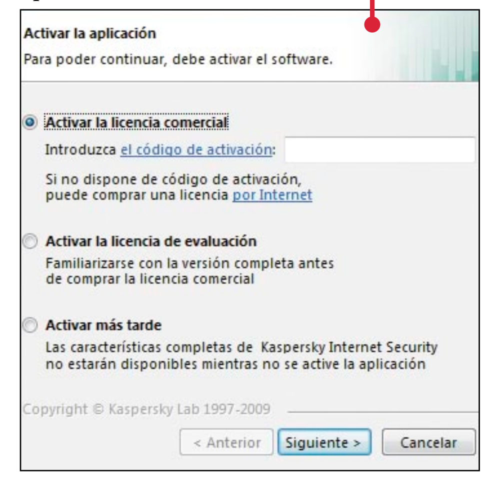


Para asegurar la mayor protección de tu equipo, Kaspersky Internet Security 2010 te ofrece multitud de posibilidades. Así, esta suite mantiene tu identidad a salvo, garantiza compras online seguras, te protege ante todo tipo de malware, salvaguarda tus conexiones wifi y favorece el normal funcionamiento del PC. Aparte, incluye un área de seguridad para supervisar la actividad de las aplicaciones. Consulta más información en www.kaspersky.com/sp

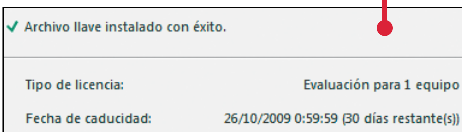
Tu zona de seguridad

Aunque Kaspersky Internet Security 2010 contiene numerosos recursos para que tu PC esté completamente protegido, es su zona de seguridad la que te permitirá gestionar tus aplicaciones y determinar el tipo de acceso que tienes a cada una de ellas, para evitar que nadie que utilice tu ordenador pueda manejar contenido poco seguro. La versión de prueba de la suite está disponible durante 30 días.

1 Cuando instales la aplicación en tu PC, el asistente te pedirá que indiques qué tipo de activación vas a realizar.



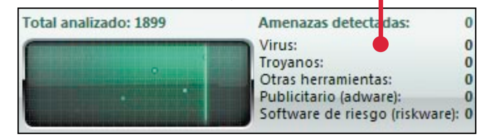
Habilita la casilla [Activar la licencia de evaluación] para poder disfrutar de la suite durante un periodo de prueba limitado y haz click en [Siguiente >]. Una ventana te indicará la fecha de caducidad de la licencia.



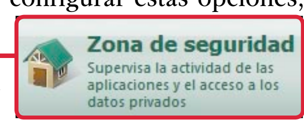
así que presiona de nuevo en [Siguiente >] y la instalación de Kaspersky Internet Security 2010 finalizará con éxito. Verás que el icono del programa se ha añadido a la barra de tareas del escritorio y deberás hacer doble click sobre él para que se muestre la pantalla principal de la aplicación.



Automáticamente, la suite comenzará a analizar tu equipo en busca de algún tipo de amenaza o código malicioso.



En el momento en el que el programa identifique la existencia de riesgos en tu ordenador, mostrará un mensaje de alerta en la parte superior de la pantalla

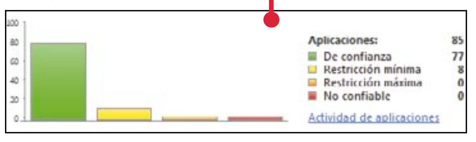


y, para solucionarlo, tendrás que presionar en el botón [Reparar ahora].

2 Junto a las opciones básicas de antivirus, Kaspersky Internet Security permite supervisar y gestionar la actividad de las aplicaciones instaladas en el ordenador, así como controlar el acceso a tus datos privados. Para configurar estas opciones, presiona en la pestaña [Zona de seguridad — Supervisa la actividad de las aplicaciones y el acceso a los datos privados] y se mostrarán todas las opciones que están asociadas a este menú.



3 En primer lugar, la función denominada [Control de aplicaciones] almacena las acciones realizadas por los programas de tu equipo y administra el acceso a los recursos. Como ves, Kaspersky Internet Security cataloga tus aplicaciones en función del grado de fiabilidad.

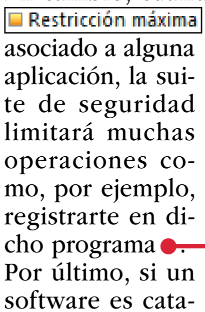


De este modo, si un programa es considerado [De confianza] significa que es seguro, y que el usuario puede acceder a él sin ningún tipo de limitación. Si tiene la denominación [Restricción mínima], por otra parte, es posible que se solicite autorización para realizar algunas acciones a través de una ventana similar a esta:

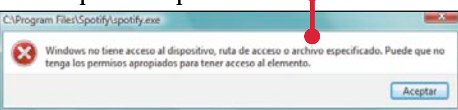




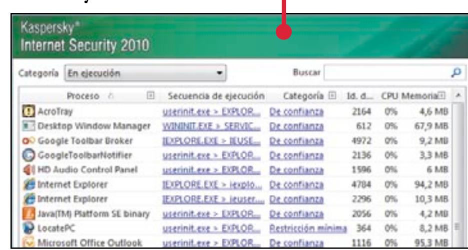
así que tendrás que presionar en [Sí — Autorizar la ejecución del programa] para poder realizar una tarea concreta. En cambio, cuando aparece el indicador [Restricción máxima] asociado a alguna aplicación, la suite de seguridad limitará muchas operaciones como, por ejemplo, registrarte en dicho programa.



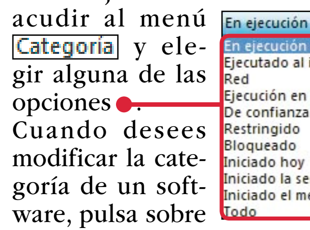

Por último, si un software es catalogado como [No confiable], entonces no será de confianza, y Kaspersky Internet Security bloqueará cualquier acción ejecutada por las aplicaciones.



4 Aunque el programa de Kaspersky otorga estas categorías en función de sus parámetros de análisis, tú puedes modificarlas según tus intereses. Para ello, haz click en el enlace [Actividad de aplicaciones] y se abrirá una nueva ventana, donde se muestran todas las aplicaciones que están ejecutándose en ese momento en tu ordenador y su clasificación.



Ten en cuenta que, si quieres visualizar también el resto de programas que no están en ejecución en ese momento, debes acudir al menú [Categoría] y elegir alguna de las opciones.

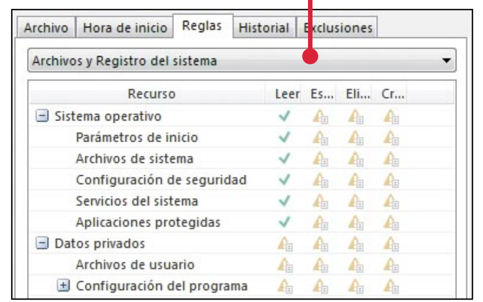


Cuando desees modificar la categoría de un software, pulsa sobre

él con el botón derecho del ratón y, en el menú que aparece, elige Cambiar estado. A continuación deberás seleccionar una de las posibilidades que se muestran, según tus intereses.

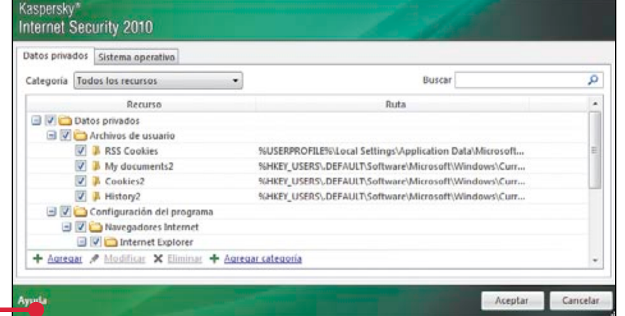
5 Dependiendo del grupo en el que se engloban las aplicaciones, tienen una serie de permisos comunes para el acceso a los recursos, aunque es posible cambiar estas reglas predefinidas. De nuevo presiona en un programa con el botón derecho del ratón y selecciona, en esta ocasión, **Reglas para aplicaciones**. La ventana que se abre a continuación te muestra información detallada sobre la aplicación, como el nivel de riesgo estimado.

Si acudes ahora a la pestaña denominada Reglas verás las acciones que están permitidas y aquellas que no.

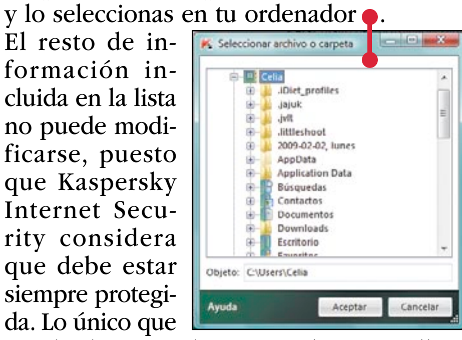


Para modificar algún permiso, pulsa en una tarea con el botón derecho del ratón y elige entre Autorizar, Denegar y Preguntar al usuario. Una vez que acabes de concretar los permisos, presiona en Aceptar y vuelve a la pantalla principal pulsando en Cerrar.

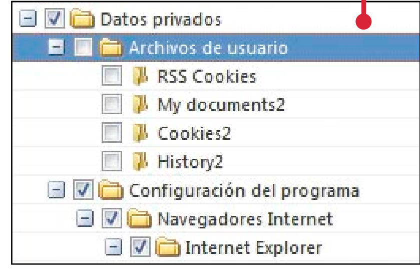
6 La zona de seguridad de Kaspersky Internet Security no sólo permite gestionar el acceso a las aplicaciones, sino también determinar la protección de datos privados para aquellas aplicaciones que necesiten confirmar la identidad del usuario. Para ello, acude al campo denominado Protección de identidad digital y presiona luego en el enlace Configuración, que desplegará una nueva pantalla con todos los servicios y aplicaciones que el programa protege por defecto.



No obstante, podrás añadir otras reglas si pinchas en la opción Agregar, eliges el tipo de recurso que quieres mantener seguro de entre las posibilidades que se muestran y lo seleccionas en tu ordenador.

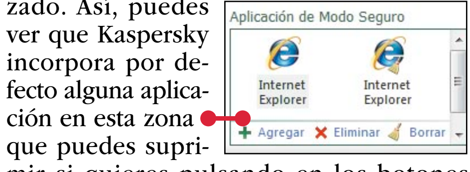


El resto de información incluida en la lista no puede modificarse, puesto que Kaspersky Internet Security considera que debe estar siempre protegida. Lo único que puedes hacer es desactivar alguna casilla si quieres renunciar a la supervisión.



Para acabar, haz click en Aceptar.

7 La última de las opciones incluidas en esta área de protección es Modo Seguro y permite ejecutar algunos programas en un espacio virtual, bloqueando el acceso a los recursos del sistema operativo y limitando así el riesgo de que el equipo se vea amenazado. Así, puedes ver que Kaspersky incorpora por defecto alguna aplicación en esta zona que puedes suprimir si quieres pulsando en los botones Eliminar o Borrar. También es posible añadir a ese listado algún otro programa presionando en la opción Agregar y eligiendo Aplicaciones, para que se muestre un amplio conjunto de programas.



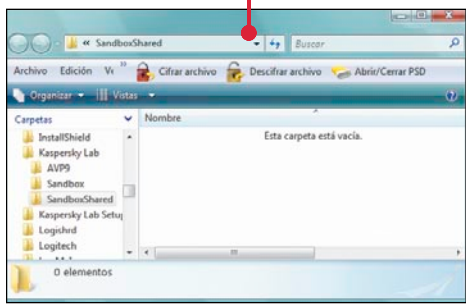


El que selecciones se agregará inmediatamente a las aplicaciones en modo seguro



y para activarlo en dicho espacio virtual deberás hacer doble click sobre él.

8 Por último, al utilizar este espacio de seguridad tienes la opción de guardar todos los archivos en un directorio que Kaspersky ha creado por defecto, y al que puedes acceder pulsando en la entrada Carpeta compartida. Sólo con pinchar sobre el enlace se abrirá el directorio en cuestión



aunque por el momento estará vacío. Para almacenar los ficheros en él, tan solo necesitarás arrastrarlos o copiarlos como haces habitualmente.

9 No olvides echar un vistazo al resto de opciones disponibles en la suite de seguridad de Kaspersky. Desde la pestaña



puedes gestionar todos los recursos necesarios para evitar infecciones en tu PC debidas a programas maliciosos, a través de tres tipos de protección: de archivos, del sistema y de la privacidad.



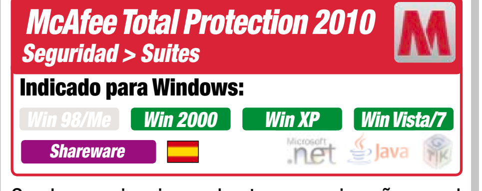
Y mediante la opción



tienes la posibilidad de iniciar cuando desees un examen del PC en busca de amenazas, con la posibilidad de elegir el tipo de análisis



De este modo mantendrás tu equipo seguro frente a cualquier amenaza.



Con la experiencia que le otorgan varios años en el ámbito de la seguridad informática, McAfee ha englobado sus más recientes y mejores herramientas antimalware en la suite Total Protection 2010. De este modo, y con una única instalación, el PC puede reforzar sus barreras digitales con un potente antivirus, firewall y antispam. Además, incluye un interesante control parental. Para más información, visita su web www.mcafeeantivirus.es

Vigila la fiabilidad de tu red

Aunque siempre viene bien disponer de un programa que defienda al ordenador ante los ataques dirigidos a la memoria o el correo electrónico, la seguridad preventiva puede ser, en ocasiones, de mayor ayuda. A partir de este supuesto, McAfee Total Protection 2010 vigila las vías de entrada de posible información dañina, ya provenga de otro terminal con el que se comparte una red local, o desde una página online que no debiera ser visitada en ningún caso. No obstante, su motor de eliminación y puesta en cuarentena de archivos dañados, también garantiza un control completo sobre cualquier tipo de amenaza residente.

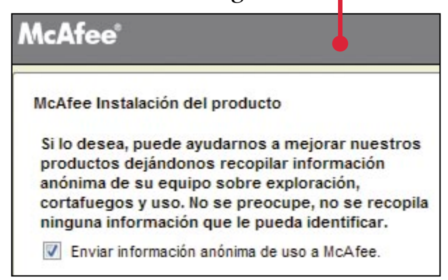
1 Antes de comenzar a ejercer su control de seguridad, esta suite realiza un chequeo rápido del equipo en busca de cualquier virus almacenado en el PC.



De este modo, se asegura la limpieza de la memoria antes de su puesta en marcha. Una vez finalizada esta operación, se procede a grabar el conjunto de archivos que forman la utilidad.

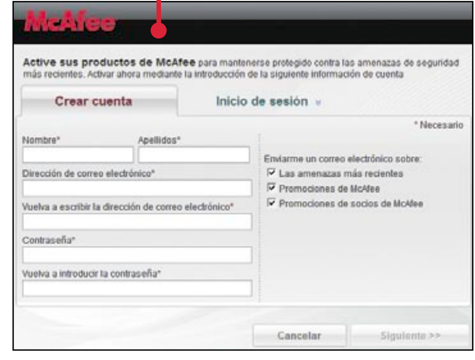
2 Como se puede observar durante su instalación

Total Protection es, en realidad, un conjunto de herramientas independientes del desarrollador, que combinan sus capacidades para obtener un resultado más fiable. No obstante, hay que recordar que la mejor manera para contrarrestar un virus pasa por enviar toda la información posible a los diseñadores de vacunas. Por este motivo, es recomendable que verifiques esta acción automática en la oportuna pantalla del asistente de configuración.



3 Sin necesidad de reiniciar el equipo, y una vez finalizada su instalación, McAfee Total Protection 2010 comienza a supervisar la seguridad del PC, algo que queda reflejado en la inclusión de su icono dentro de la barra de tareas del equipo.

Si haces click sobre este símbolo, al instante aparece una pantalla en donde introducir algunos datos personales para activar el programa.

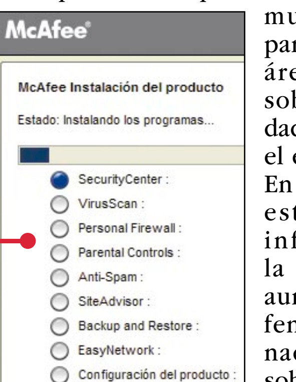


Si deseas hacer este registro previo en otro momento, presiona el botón Cancelar y, en la ventana que aparece después



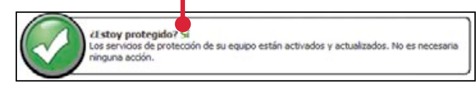
pulsa la entrada Recordármelo más tarde.

4 En cuanto que se abre la interfaz principal de esta aplicación



muestra en su parte superior un área que alerta sobre la seguridad instaurada en el equipo. En el caso de que este indicador informe sobre la necesidad de aumentar las defensas del ordenador, haz click sobre el botón.

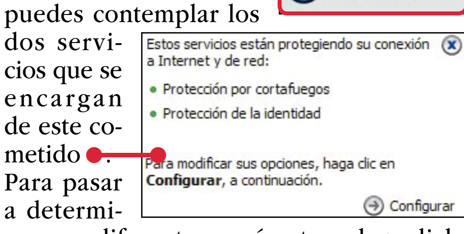
Con esta operación, la utilidad busca aquellos parámetros que, por defecto, debieran estar habilitados, y los activa al momento, lo que hace variar su barra de estado inmediatamente.



Seguridad proactiva para la red

La mejor solución para que tu ordenador esté a salvo mientras navegas por Internet es contar con una buena defensa online.

1 Además de contar con una importante defensa para antivirus, software espía y protección general para los registros operativos de Windows, opciones que puedes encontrar listadas tras pulsar el botón McAfee Total Protection 2010 dispone también de una potente salvaguarda para las áreas críticas de comunicación con otros equipos: Internet y la red local. De este modo, si desde la interfaz principal presionas la entrada puedes contemplar los dos servicios que se encargan de este cometido.

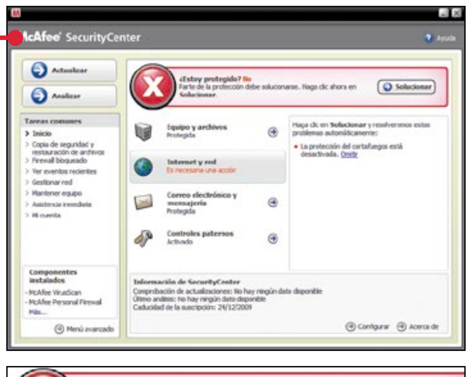


Para pasar a determinar sus diferentes parámetros, haz click sobre la función Configurar.

2 Ya dentro del menú de configuración de Internet y redes



se distinguen hasta cuatro apartados diferentes para definir sus características. De

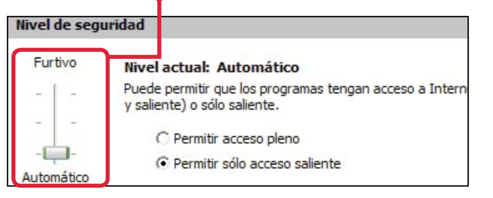


esta forma, en primer lugar la sección especial sirve para activar el cortafuego. De igual modo, si deseas precisar con mayor detalle su uso, presiona el botón Avanzadas... para que, poco después, aparezca la pantalla .

La protección por cortafuegos está activada
Activado — Su equipo está protegido contra intrusiones y conexiones de Internet no deseadas.
Desactivado — Un cortafuegos protege el equipo de intrusiones y de trafico de red no deseado, además de ayudar a gestionar las conexiones de Internet entrantes y salientes.
Avanzadas...

Nivel de seguridad
Furtivo — Nivel actual: Automático
Puede permitir que los programas tengan acceso a Internet completo (entrante y saliente) o sólo saliente.
Permitir acceso pleno
Permitir sólo acceso saliente
Automático

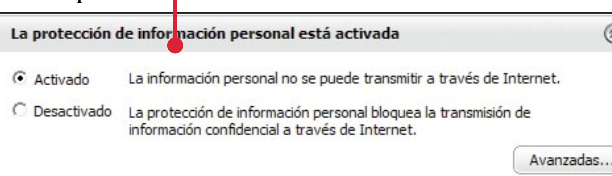
Una de las herramientas que ahora puedes usar es una cómoda barra de desplazamiento vertical. Ésta se encarga de establecer el nivel de restricción en el traslado de datos online .



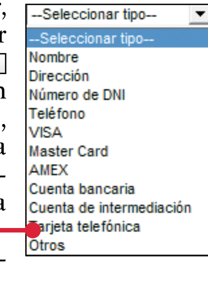
Configuración de seguridad
Habilite la protección al iniciar Windows
Permitir solicitudes de ping ICMP
Activar rastreo de puertos UDP

Además, gracias a las funciones verificables es posible ejecutar esta barrera desde el mismo arranque del sistema operativo.

3 Otra de las variantes de seguridad que tienen que ver con la navegación por el ciberespacio es la que aparece reflejada en el apartado .



Gracias a ella, y siempre que se encuentre activada, la información personal no se puede transmitir sin autorización previa a través de Internet. Asimismo, para introducir los datos que quieres reservar sólo para uso particular, prueba ahora a pulsar su entrada Avanzadas... seguida de la función Agregar. Por último, elige la categoría de la información que quieres añadir mediante la pestaña desplegable y rellena el correspondiente formulario

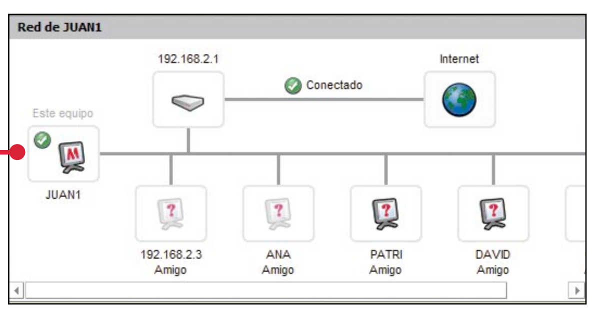




4 Paralelamente, aunque los ordenadores conectados a una misma red tienen la capacidad inicial de compartir todo tipo de datos, puede que te interese restringir el acceso a varios de los terminales de tu entorno. Si ésta es tu intención, busca en la interfaz principal de McAfee Total Protection la columna correspondiente a las aplicaciones .

Tareas comunes
Inicio
Copia de seguridad y restauración de archivos
Firewall bloqueado
Ver eventos recientes
Gestionar red
Mantener equipo
Asistencia inmediata

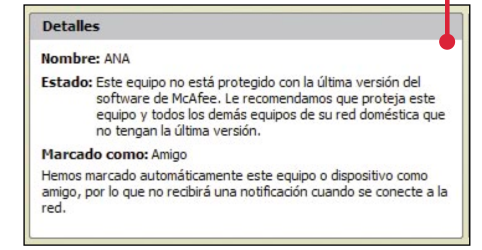
Acto seguido, selecciona, con la ayuda del cursor, la entrada Gestionar red. Como ahora puedes contemplar, un nuevo diagrama de relación establece el entramado de tu actual red local .



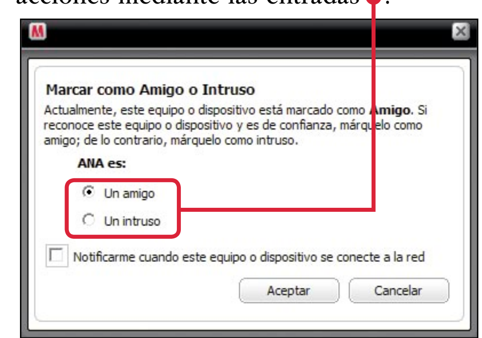
Ten en cuenta que, para modificar los atributos de todos y cada uno de los equipos incluidos en ella, has de acudir al amplio listado de funcionalidades .

5 La primera de estas herramientas se denomina Actualizar el mapa de la red y, como su propio nombre indica, se encarga de poner al día todos los puestos de trabajo de la red local. Una vez utilizada esta aplicación, selecciona con el cursor cualquier ordenador cuyo perfil te interese definir. Al hacer esto, el programa aporta automáticamente un resumen de su condición actual mediante la sección especial de texto ampliado .

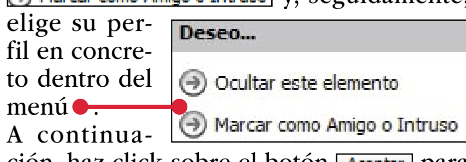
Deseo...
Actualizar el mapa de la red
Cambiar el nombre de la red
Mostrar elementos ocultos
Dejar de confiar en esta red
Dejar de detectar nuevos amigos



Asimismo, también permite realizar dos acciones mediante las entradas .



6 Al determinar si un ordenador tiene la condición de Amigo o de Intruso, se le está otorgando la posibilidad o no de poder comunicarse libremente con todos los recursos compartidos de nuestro PC, incluida la información contenida en los discos duros cuyo acceso no esté restringido por el sistema operativo. Sabiendo esto de antemano, para cada uno de los equipos de la red pulsa la entrada Marcar como Amigo o Intruso y, seguidamente, elige su perfil en concreto dentro del menú .



A continuación, haz click sobre el botón Aceptar para validar la nueva configuración.

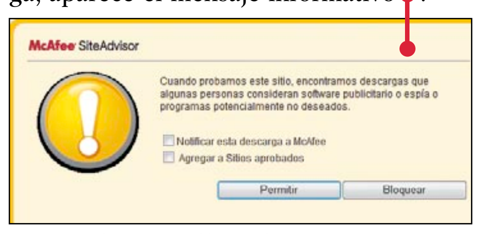
7 No obstante, McAfee Total Protection 2010 no sólo se encarga de redes locales, sino que también supervisa la navegación y las descargas desde Internet. De esta forma, puedes poner su control de seguimiento haciendo una búsqueda simple en el navegador de Internet Explorer. Ahora observa cómo, acompañando cada resultado, aparece un símbolo de verificación, incluido por el propio entorno de seguridad .

Rebelion en la Granja Georgo Orwell (1 de7)
9 min
www.youtube.com

Al pausar el ratón sobre estos iconos, un bocadillo resume sus características de fiabilidad para poder visitar sin miedo sus contenidos webs .



8 Por último, al intentar descargar cualquier documento desde Internet, en caso de dudas sobre el origen de la descarga, aparece el mensaje informativo .



Recuerda que, llegados a este punto, puedes optar por verificar las diferentes funciones Notificar esta descarga a McAfee o Agregar a Sitios aprobados, antes de proseguir con el tránsito de información.

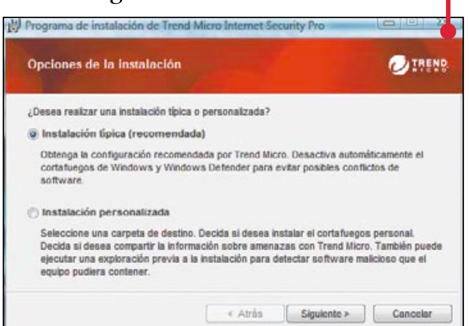


Gran parte de las amenazas que pueden desestabilizar el equilibrio de un ordenador provienen de Internet. Esto se debe a que, en muchas ocasiones, las barreras establecidas para navegar por el ciberespacio no son lo suficientemente potentes como para poner freno al malware de última generación. Para este fin, Trend Micro Internet Security Pro 2010 aporta sus herramientas continuamente actualizadas desde la web. http:/es.trendmicro.com

A prueba de malware online

¿Por qué arriesgarse a visitar una página web potencialmente peligrosa para nuestro PC, si es posible averiguar previamente su fiabilidad? Con Trend Micro Internet Security Pro 2010 tan solo es necesario actualizar su extensa base de datos y ajustar sus múltiples parámetros para empezar a sentirse a salvo. Además, entre sus prácticas aplicaciones se incluye un completo analizador de memoria que se anticipa a cualquier tipo de virus encubierto.

1 Durante la instalación de esta suite, su asistente permite optar entre dos posibles configuraciones mediante el menú.



No obstante, y como su propio texto indica, la variante más recomendada es la que lleva por título [Instalación típica (recomendada)]. La principal ventaja de esta selección radica en que, a través de ella, se desactivan automáticamente los dos sistemas de seguridad por defecto del sistema operativo: el cortafuegos de Windows y el programa Windows Defender. De igual forma, en el caso de que no elijas esta vía de grabación en el disco duro, asegúrate de desinstalar manualmente ambas utilidades, ya que pueden impedir el buen funcionamiento del entorno de seguridad de Trend Micro.

2 Otra de las funciones que te permite realizar el asistente inicial es la actualización de su base de datos, para incluir en ella las últimas medidas contra todo tipo de virus infiltrado.



A pesar de que se trata de una operación que, posteriormente y de forma periódica realizará la herramienta, es conveniente activar su puesta al día antes de que comience la supervisión del programa. Para ello, pulsa el botón [Actualizar ahora]. Poco después, todos y cada uno de sus apartados entrarán en contacto con la página del desarrollador para descargar los últimos contenidos antimalware.



3 Esta versión de prueba necesita una activación que se verifica desde la página web del fabricante. Para realizarla, incluye en el breve formulario



una cuenta personal de correo electrónico y presiona la entrada [Siguiente >]. Tras unos segundos de comprobación, recibirás la confirmación del registro mediante la ventana informativa.



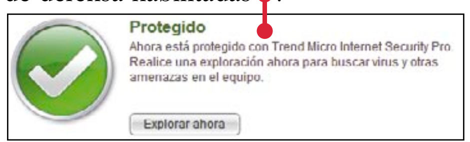
Por último, cierra el asistente de instalación pulsando el botón [Finalizar].

4 La primera prueba de que la suite Trend Micro Internet Security Pro 2010 está en funcionamiento es la aparición de su icono en la barra de herramientas. Desde este mismo momento, todas sus barreras se activan para restringir cualquier tipo de acceso inadecuado y ataques de malware. De este modo, para acceder a su interfaz principal tan solo es necesario hacer doble click sobre su correspondiente símbolo.

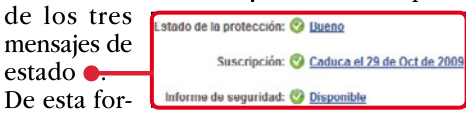
5 Es probable que la configuración inicial de la aplicación no se ajuste al nivel de seguridad óptimo. De ser así, un primer mensaje de alarma encabeza su ventana con la información.



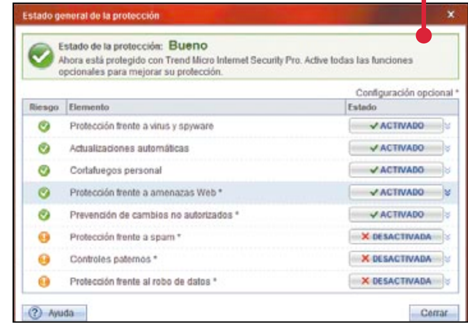
No obstante, a pesar de este aviso, la utilidad aporta la función [Solucionar ahora] para poder corregir al instante cualquier parámetro que no permita establecer una defensa media aceptable. Así, tras pulsar su botón correspondiente, puedes observar cómo el estado varía para reflejar la correcta configuración de todas las medidas de defensa habilitadas.



6 Para aportar una mayor información acerca de su funcionamiento, Trend Micro Internet Security Pro 2010 dispone de los tres mensajes de estado.



De esta forma, la primera de ellas simplifica el nivel general de la suite [Bueno], aunque al hacer click sobre su texto enumera una a una todas las funciones que forman el programa y generan su actual situación.



Hay que señalar, llegados a este punto, que la principal ventaja de este apartado adicional no es otra que la de aportar un listado claro y conciso de todas las herramientas disponibles y, sobre todo, de su estado actual. Una vez explicado esto, ten en cuenta que si el símbolo que antecede a la herramienta es [✓], entonces la utilidad está completamente activada. Después, en el caso de que aparezca el icono [!], se trata de programas cuya activación no se considera obligatoria para prevenir ataques malintencionados, aunque sí muy recomendables. En tercer y último lugar, si el icono previo es [✗], entonces la activación del programa resulta vital para la fiabilidad del equipo, y todavía se encuentra pendiente de ser habilitada. Igualmente, si necesitas leer una pequeña explicación

del estado de cada utilidad, al hacer click sobre el indicador lateral ☑ aparecerá para cada caso una breve línea informativa de texto adicional ●.

Riesgo	Elemento	Estado
✔	Protección frente a virus y spyware	✔ ACTIVADO
	Ahora está protegido frente a virus, gusanos, troyanos, spyware y otras amenazas relacionadas.	

7 La segunda línea que verás tiene que ver con el tiempo que falta para finalizar la licencia de uso de la suite Suscripción: ✔ Caduca el 29 de Oct de 2009. Al hacer click sobre su enunciado aparece una nueva ventana emergente ●



que presenta los datos del registro, y permite comprar el programa definitivo, cambiar el número de serie o recomendar la aplicación a otro usuario a través de sus correspondientes enlaces.

8 La última frase explicativa de la interfaz principal Informe de seguridad: ✔ Disponible sirve como nexo para acudir al informe de las exploraciones realizadas con éxito en el PC hasta la fecha ●.



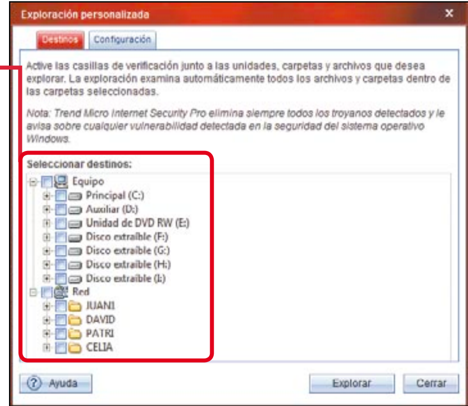
Sin embargo, para poder sacar partido a este apartado, primero debes haber realizado unos cuantos análisis previos para detectar virus de todo tipo en la memoria de tu ordenador.

9 Si ahora quieres realizar un chequeo de la memoria para limpiarla de posibles infecciones, presta atención al botón Explorar ahora. De hecho, puedes utilizar este control de tres formas diferentes si accedes a las correspondientes entradas tras pulsar su pestaña desplegable ●.

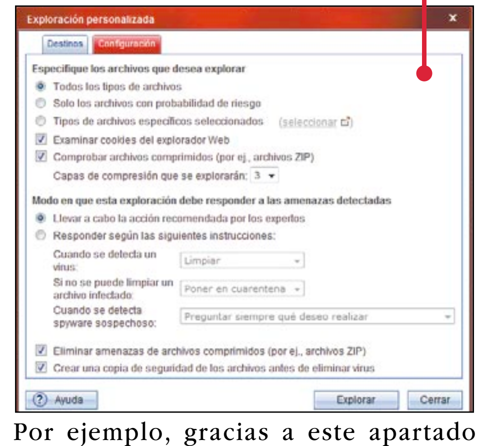
Explorar ahora
Exploración rápida
Exploración completa del sistema
Exploración personalizada...

No obstante, de las tres variantes disponibles, la que mejor permite configurar la búsqueda es la que lleva por nombre Exploración personalizada....

10 El menú de la exploración personalizada se encuentra dividido en dos pestañas diferentes. Así, por un lado la denominada Destinos muestra en su interior todas las ubicaciones que pueden ser marcadas para analizar durante la búsqueda de malware en tu equipo ●.

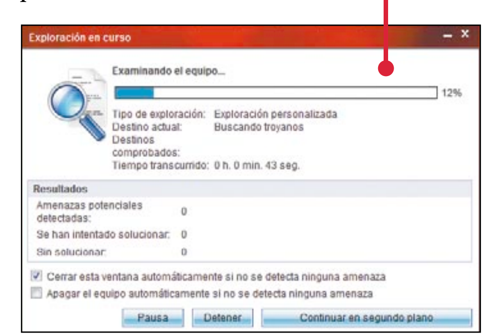


Luego, la pestaña Configuración presenta una gran variedad de opciones para realizar un chequeo justo a la medida que más convenga al usuario ●.



Por ejemplo, gracias a este apartado se pueden examinar los archivos que se encuentren comprimidos en formato Zip, marcando la casilla titulada ☑ Comprobar archivos comprimidos (por ej., archivos ZIP). También es posible simplificar el análisis dirigiendo el foco de atención sobre aquellos ficheros que realmente tienen riesgo de haber sido corrompidos. Para este fin, selecciona la utilidad ◯ Solo los archivos con probabilidad de riesgo antes de validar la nueva configuración presionando sobre el botón Explorar.

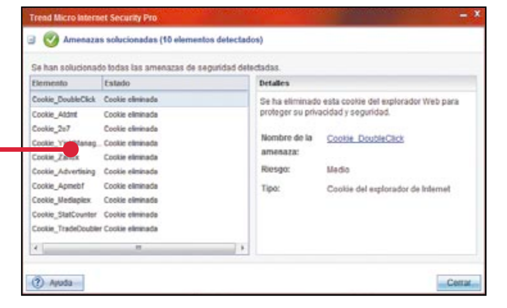
11 Una vez que comienza, el análisis de la memoria revisa las direcciones previamente definidas a la búsqueda de posibles amenazadas residentes ●.



Cabe destacar que, para señalizar el avance de este proceso, en la ventana de la exploración se va rellenando una barra horizontal de izquierda a derecha, al mismo tiempo que se revisan los ficheros potencialmente peligrosos, uno a uno.

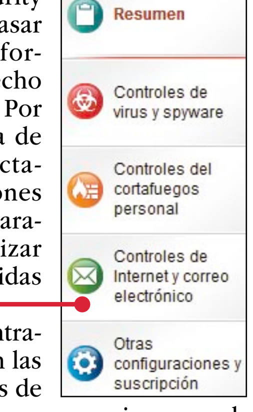
12 Como resultado de esta operación, Trend Micro Internet Security Pro 2010 se encarga de mostrar un resumen de todos los elementos que han sido detectados, así como el método que se ha utilizado para su neutralización ●. De hecho, si en el listado situado a la izquierda se elige, con la ayuda del cursor, uno de los registros dañinos, a la derecha se expone el nombre de la amenaza, su nivel de peligro potencial y el tipo del virus que oculta en su interior ●.

Detalles
Se ha eliminado esta cookie del explorador Web para proteger su privacidad y seguridad.
Nombre de la amenaza: Cookie_DoubleClick
Riesgo: Medio
Tipo: Cookie del explorador de Internet



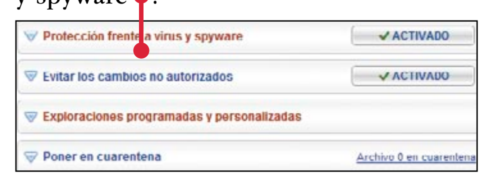
Para salir de este apartado pulsa el botón Cerrar.

13 Según te vayas familiarizando con los análisis habituales de Trend Micro Internet Security Pro 2010, podrás pasar a descubrir otras formas de sacar provecho a sus aplicaciones. Por ejemplo, una forma de poder acudir directamente a sus secciones principales por separado consiste en utilizar las funciones recogidas en el recuadro ●.



Cada una de sus entradas se identifica con las opciones principales de la suite, con lo que con presionar cualquiera de ellas se pueden configurar al instante.

14 Prueba ahora a pulsar la entrada Controles de virus y spyware ●. Justo después se presentan, en el lado derecho de la ventana, cuatro apartados que se identifican con las herramientas que esta suite utiliza para combatir virus y spyware ●.



Para activar o desactivar cualquiera de las utilidades aquí descritas, tan solo es necesario pulsar el botón ✔ ACTIVADO. Además, si

presionas el símbolo de principio de línea [icono], cada sección se amplía para mostrar nuevas opciones de configuración.

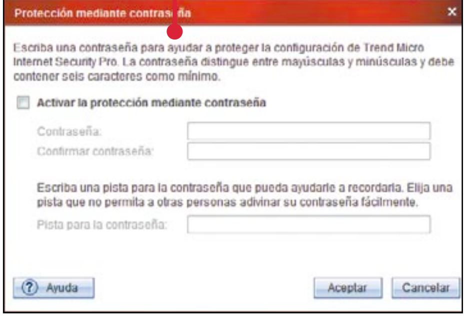
Evitar los cambios no autorizados ✓ ACTIVADO
Cuando está activado, esta función puede proteger el equipo frente a cambios no autorizados realizados en el sistema operativo o en los programas importantes.
Configuración · Lista de excepciones

15 Siguiendo estas pautas, puedes también visitar el apartado dedicado al firewall, mediante el botón de función [Controles del cortafuegos personal] o el del filtro antispam, con la entrada [Controles de Internet y correo electrónico]. Asimismo, desde el mismo recuadro puedes utilizar el control [Otras configuraciones y suscripción] para acceder a la configuración más avanzada del programa. En su apartado posterior correspondiente encontrarás todo tipo de ajustes, incluido uno de especial interés si quieres preservar tu propio perfil de seguridad.

16 En realidad, se trata de la función avanzada

Contraseña
Haga clic en Configuración para definir una contraseña y evitar que otros puedan realizar cambios en Trend Micro Internet Security Pro sin su permiso.
Configuración

la cual se encarga de definir una contraseña para que otros usuarios no puedan realizar cambios en Trend Micro Internet Security 2010 sin tu permiso. De este modo, haz click sobre el vínculo [Configuración], y utiliza el formulario que aparece justo a continuación para introducir una clave, repetirla para su verificación y escribir alguna pista que te ayude a recordarla en caso de olvido.



Una vez que hayas marcado la casilla [Activar la protección mediante contraseña] y pulses el botón [Aceptar], este control de acceso entrará en funcionamiento.

17 Aunque esta suite de seguridad dispone de muchas defensas para eliminar cualquier tipo de virus infiltrado en la memoria del ordenador, también permite una supervisión muy completa de la red local y de los accesos a Internet. Para descubrir sus ventajas, acude a la pestaña superior [Mi red doméstica]. Tras hacer esto, aparece la pantalla de configuración.



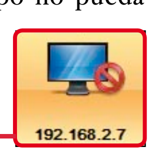
Asimismo, resulta recomendable que, antes de activar alguna de sus prácticas utilidades, pulses el botón [Abrir mapa de red]



para poder visualizar con todo detalle la estructura de tu red local.

18 Cuando hayas comprobado cuáles son los equipos con los que compartes red local, si no tienes claro hasta qué punto quieres compartir tu información con sus usuarios puedes presionar el acceso [¿Desea fortalecer aún más su red?] para averiguar más datos en un práctico tutorial. Sin embargo, con que selecciones con el cursor uno de los iconos del puesto de trabajo podrás definir tu relación de transferencia de documentos con él.

Así, si deseas que un equipo no pueda vincularse a tu PC, no tienes más que señalar la sentencia [Bloquear este equipo]. Acto seguido, su icono varía para mostrar la nueva imagen.

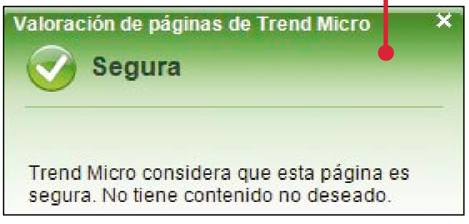


Internet Security Pro — Mi equipo · Mi red doméstica · Ayuda y asistencia
Total de equipos detectados: 4 · Actualizar
192.168.2.7 — Conexión a Internet: En línea · Dirección IP: 192.168.2.7 · Dirección MAC: 00:19:E0:79:4A:FD · Estado: No conocido (Detalles)
Acciones que puede realizar ahora: Cómo proteger este equipo · Activar el control remoto · Bloquear este equipo · ¿Necesita ayuda?
Internet · Dispositivo de ... · JUAN1 (este equipo) · 192.168.2.7 · ANA · DAVID

19 En relación a la navegación a través de Internet, esta extensa aplicación también tiene en cuenta los riesgos potenciales que generan los portales de dudosa reputación. Prueba de ello es el analizador online que se instala automáticamente en la parte superior del explorador.

TREND MICRO · Página segura

Su funcionamiento es bien sencillo: varía su estado basándose en la credibilidad que le conceda a la página activa en cuestión.



Además, siempre se puede comprobar la fiabilidad de un sitio web antes de visitarlo mediante los iconos representativos añadidos en el margen izquierdo.



20 Por último, en el caso de querer establecer una conexión inalámbrica, puedes reforzar el enlace mediante el recurso que se activa tras pulsar sobre el icono [icono]. Tal y como explica la siguiente ventana informativa y emergente



se trata de una herramienta que combina su uso con el asesor de redes inalámbricas de Microsoft. Para activarlo presiona el botón [Aceptar]. Desde ese mismo momento, cualquier enlace inalámbrico que se realice desde el equipo ve reforzada su conexión con un doble sistema de defensa: el que aporta el propio sistema operativo, más el que suma Trend Micro Internet Security Pro 2010. Pronto descubrirás que esta combinación no sólo blinda la línea ante intrusos, sino que, además, optimiza el sistema.

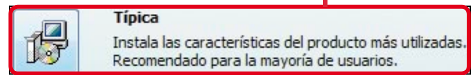


Además de proteger tu equipo frente a cualquier amenaza, la suite de seguridad BitDefender Total Security 2010 cuenta con útiles herramientas como un optimizador del registro y del disco duro, un asistente para crear copias de seguridad o un gestor de la red. Asimismo, la aplicación te permite mantener seguros tus archivos a través de su módulo de cifrado. Encontrarás más información al respecto en la página web www.bitdefender.es

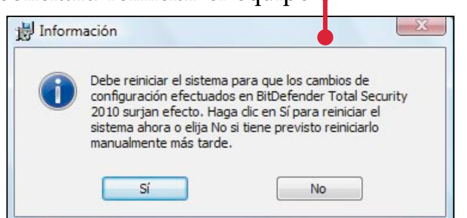
Tus documentos a salvo

De todas las opciones de esta plataforma de seguridad, una de las más novedosas es su función de almacenamiento, que no sólo te permite realizar backups para restaurarlos posteriormente, sino también cifrar tus documentos con claves para que estén a salvo de posibles intrusiones. Y, con el completo asistente de instalación y configuración, no tendrás problemas para proteger tu equipo en todo momento. Puedes probar la suite durante 30 días.

1 Durante la instalación del programa tienes la posibilidad de seleccionar un proceso personalizado, para que ejecutes todos los componentes que desees, o uno automático. Elige la opción



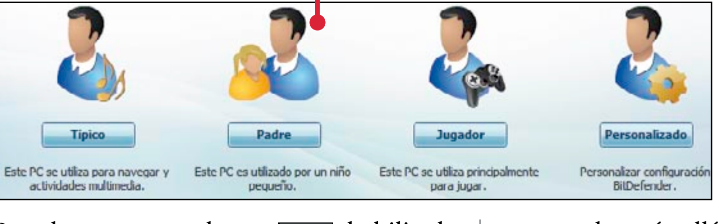
y, cuando finalice la tarea, una pantalla te solicitará reiniciar el equipo



de modo que haz click en Sí. Una vez que el PC se encienda de nuevo, se abrirá el asistente y deberás confirmar que quieres continuar con la versión de prueba de la suite, pulsando para ello sobre Deseo evaluar BitDefender. Presiona en Siguiente y una nueva pantalla te informará de que, para tener acceso a las actualizaciones antimalware y al soporte técnico, será necesario que crees una cuenta en BitDefender. Puedes hacerlo en este momento si habilitas la opción Crear una nueva cuenta, indicas tu dirección de contacto y una clave y pinchas en Crear. No obstante, si quieres dejarlo para más adelante pulsa en la opción Registrar más tarde. Para acabar la instalación, haz click en Finalizar.

Dirección de e-mail:
Contraseña: ******** Confirmar contraseña: ********
Opciones de Correo: Enviarme todos los mensajes

2 Es posible que el programa de BitDefender reconozca la existencia de una conexión local y te pida que elijas el tipo de red que empleas en el equipo: una pública, por lo que deberás marcar la opción Esta es una red de un campus universitario o una red pública, o bien una conexión privada, y en este caso tendrás que asegurarte de activar la casilla Esta es una red doméstica, de oficina o una red de confianza. Presiona, a continuación, en Aceptar. Inmediatamente se abrirá un asistente de configuración para que selecciones el perfil de usuario que tienes, que determinará la interfaz que vas a utilizar



Por el momento pulsa en Típico, habilita la casilla Este equipo es un portátil en caso de que sea un portátil, marca Este equipo está en una red para tener acceso al módulo de administración de red y haz click en Siguiente.

3 BitDefender Total Security 2010 te permite elegir el nivel de complejidad que tendrá la interfaz. Si marcas Básico, el programa tomará todas las decisiones por ti. Con Intermedio, por otra parte, podrás realizar las acciones más importantes. Mientras que si eliges Avanzado, serás el encargado de decidir todas las operaciones de la suite. Por ahora, hasta que te familiarices con el programa, puedes utilizar el nivel Intermedio. El asistente te permite elegir si quieres llevar a cabo un análisis del PC en busca de amenazas activando la casilla Actualizar BitDefender y realizar un análisis de sistema, así como concretar si deseas realizar un examen diario del equipo y a qué hora

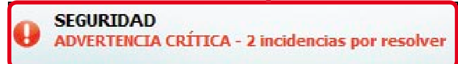


Por último, haz click en Finalizar.

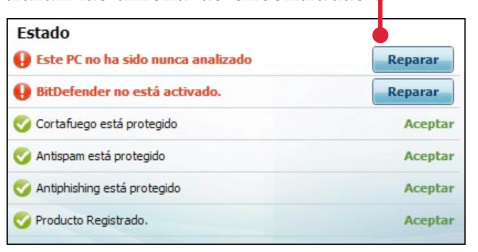
4 Una vez configurado e instalado el programa, verás que su icono aparece en la barra de tareas de tu escritorio



Debes pulsar dos veces sobre él para que se despliegue la pantalla principal. Si no has realizado anteriormente el análisis, es posible que aparezca alguna alerta avisándonte de los riesgos



De hecho, si pulsas en SEGURIDAD, se mostrarán las amenazas encontradas



y podrás solucionarlas presionando en el botón Reparar.

5 Aunque BitDefender Total Security es una suite de seguridad, en su interior contiene una serie de funciones que van mucho más allá de un mero antivirus. Así, una de las grandes posibilidades de este programa es su área de



donde son varias las acciones que puedes llevar a cabo.

Tareas Rápidas
Crear Copia
Blindar Archivo
Desblindar Archivo
Ver Blindaje
Bloquear Blindaje

6 Por una parte, es posible realizar backups para mantener a salvo los datos de tu ordenador. Para ello, haz click sobre el botón Crear Copia y se desplegará un nuevo asistente, de modo que pulsa ahora en Siguiente >. Tienes la opción de elegir



si quieres que el backup englobe todos los ficheros del PC, o bien seleccionar



para almacenar sólo los archivos que te interesen. En este caso, además, puedes



determinar qué tipo de ficheros quieres copiar, simplemente activando las casillas correspondientes desde el asistente.



Pincha en Siguiente > y, a continuación, determina si guardarás el backup en el ordenador, en un dispositivo extraíble o en un servidor.

Copiar datos en mi equipo
Copiar datos en mi memoria USB
Copiar datos en una ubicación de la red
Copiar datos en CD/DVD
Copiar datos en un servidor FTP

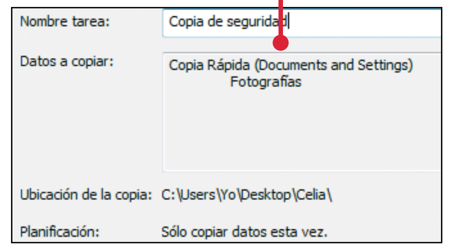
Si escoges la opción Copiar datos en mi equipo, haz click luego sobre Seleccionar ubicación y elige una localización concreta en tu PC. Pulsa en Siguiente >, determina el momento en el que se hará la copia de seguridad.

Sólo copiar los datos esta vez
Copiar los datos en momento que especifique

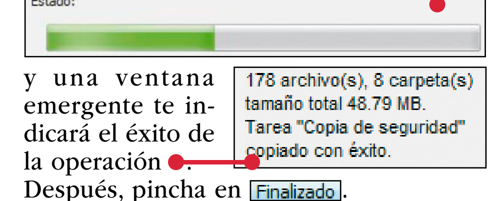
presiona una vez más en Siguiente > y, en la ventana que se muestra, otorga un nombre al archivo para poder encontrarlo después.

Nombre tarea: Copia de seguridad

Tras comprobar que los datos que has determinado son correctos

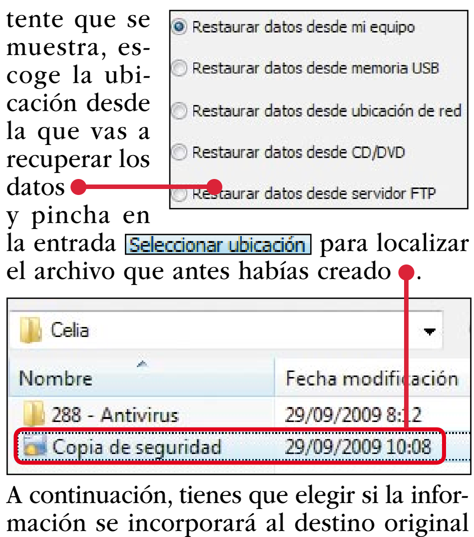


sólo tendrás que pinchar en Iniciar Copia para que comience el proceso. Verás su avance en la parte inferior de la pantalla



y una ventana emergente te indicará el éxito de la operación. Después, pincha en Finalizado.

7 Como una vez realizado el backup te será muy útil saber cómo recuperarlo, debes acudir nuevamente al menú ALMACENAMIENTO y, en la función Crear Copia pulsar sobre ▼ y elegir la opción Restaurar Copia. En el asistente que se muestra, escoge la ubicación desde la que vas a recuperar los datos



y pincha en la entrada Seleccionar ubicación para localizar el archivo que antes habías creado.

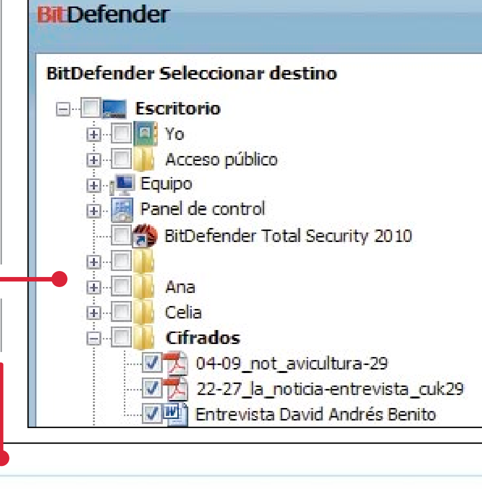
A continuación, tienes que elegir si la información se incorporará al destino original Restaurar la copia en su ubicación original o a otro distinto Restaurar la copia en una ubicación diferente; y si recuperarás todos los archivos, pulsando en Restaurar todos los datos o sólo los que te interesen, desde Restaurar determinados archivos. Cuando pulses en favor, seleccio se iniciará la restauración, y una ventana emergente te avisará una vez que finalice.

177 archivo(s), 8 carpeta(s) tamaño total 48.54 MB. Tarea "Copia de seguridad (Tarea Temporal)" restaurado con éxito.

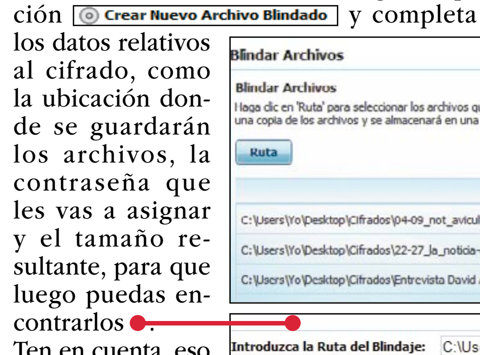
Cifrado de archivos

Aparte de realizar copias de seguridad, la opción de almacenamiento de BitDefender Total Security 2010 incluye otra función de gran utilidad: permite blindar archivos con contraseñas para que nadie pueda acceder a su contenido. Esta opción de cifrado no borrará los ficheros del disco, sino que realizará una copia y los almacenará en una ubicación con clave.

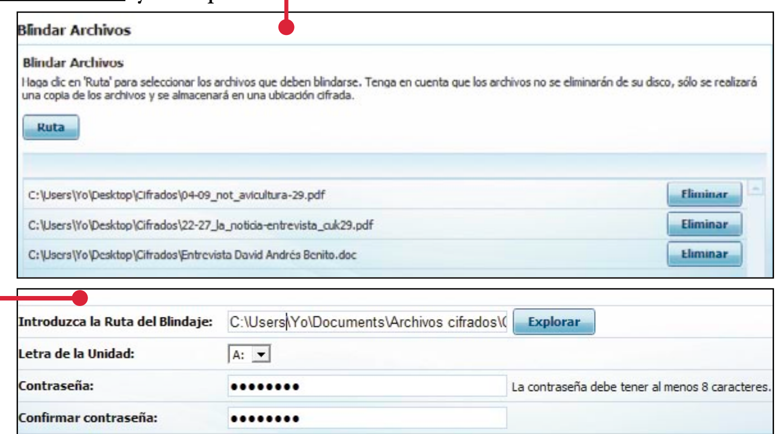
1 Para empezar a cifrar alguno de tus documentos acude al botón Blindar Archivo presiona luego sobre Ruta para seleccionar los ficheros en cuestión



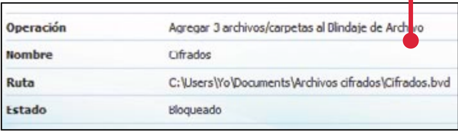
y haz click en Aceptar. Los archivos que hayas marcado se añadirán inmediatamente a la pantalla del programa.



Pincha en el botón Siguiente, elige la opción Crear Nuevo Archivo Blindado y completa los datos relativos al cifrado, como la ubicación donde se guardarán los archivos, la contraseña que les vas a asignar y el tamaño resultante, para que luego puedas encontrarlos.



Ten en cuenta, eso sí, que si blindas varios documentos al mismo tiempo, todos ellos se comprimirán en un único archivo cifrado. Revisa, a continuación, las opciones seleccionadas



y, si estás conforme con los datos, pincha en el botón Siguiente. En unos segundos el cifrado se llevará a cabo y tan solo tendrás que pulsar en Finalizar.

2 Puedes comprobar los archivos que has protegido con contraseña pulsando en la función Ver Blindaje de modo que se muestren en una nueva ventana.

Nombre del Blindaje de Archivo
C:\Users\Yo\Documents\Archivos cifrados\Cifrados.bvd

Cuando quieras abrir alguno de los ficheros que has cifrado, únicamente tendrás que localizarlo en la ruta donde lo guardaste antes, hacer doble click sobre él y escribir la clave que introdujiste para ese archivo. De este modo, la suite de BitDefender te permite tener protegidos todos tus documentos sólo con unos simples pasos, para que así ningún otro usuario pueda modificar la información, a menos que le autorices a través de la contraseña.

La ruta completa del blindaje de Archivo en disco (incluyendo el nombre del archivo y la extensión): C:\Users\Yo\Documents\Archivos cifrados\Cifrados.bvd
Letra unidad: L: Contraseña: ••••••••



Conseguir un entorno en red más seguro, sin disminuir el rendimiento del equipo. Éste es el principal objetivo de Fortinet FortiClient 2010, una aplicación gratuita y completa a la hora de enfrentarse a cualquier amenaza de malware. Entre sus ventajas, destaca la posibilidad de restringir la entrada y salida de información de un programa, sin afectar al funcionamiento del resto. Si deseas conocer más información, entra en www.forticlient.com

La red más segura

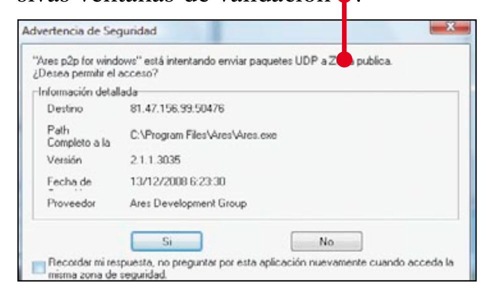
Aunque a primera vista pueda parecer que se trata de una herramienta algo técnica, FortiClient 2010 ha sido optimizada para poder aportar un alto nivel de seguridad, sin restar recursos al procesamiento, de todo tipo de equipos. Además de esta clara ventaja en comparación con otros programas similares, la solución también hace hincapié en el seguimiento y control de la información compartida con otros ordenadores, todo ello con tal de no filtrar ningún tipo de virus.

1 Durante el principio de la instalación de esta suite, su asistente se encarga de revisar cuáles son las características del sistema, para así poder optimizarlas a continuación.

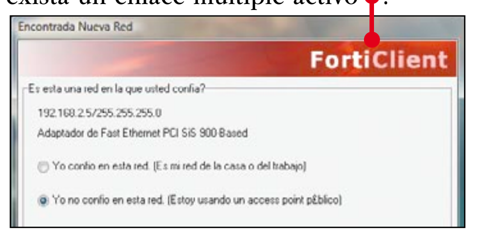


No te preocupes si esta operación de chequeo tarda varios minutos en realizarse. En realidad, aunque pueda parecer mucho tiempo empleado en un paso intermedio, pronto comprobarás cómo cada instante utilizado en esta tarea ha servido para conseguir un claro avance del rendimiento general del ordenador.

2 Si tienes instalados en el equipo otros programas que comparten y reciben información constantemente desde la red, FortiClient solicita para cada caso el permiso para su tránsito, a través de las sucesivas ventanas de validación.

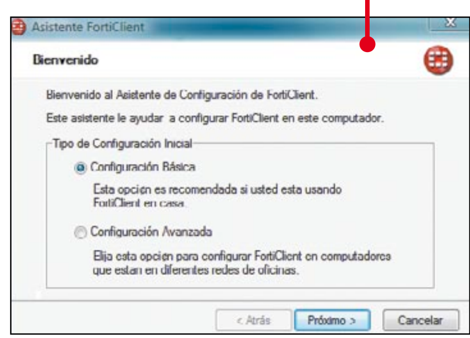


3 Después, la utilidad detecta cuáles son las redes operativas que se encuentran conectadas al ordenador. Por lo general, un equipo suele pertenecer a una única red, aunque puede darse el caso de que exista un enlace múltiple activo.



De esta forma, si estás utilizando una red de confianza para conectar tu ordenador a Internet, marca la opción verificable [Yo confío en esta red. (Es mi red de la casa o del trabajo)]. Si justo es lo contrario, señala la sentencia [Yo no confío en esta red. (Estoy usando un access point pŭblico)] antes de pulsar [Aceptar].

4 Para poder ajustarse a las preferencias del usuario, el asistente de configuración de FortiClient distingue dos modalidades de instalación diferentes.

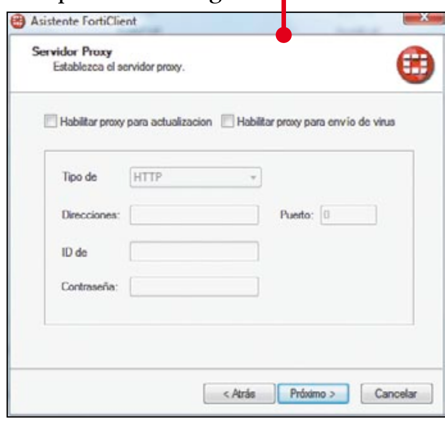


En primer lugar, la variante denominada [Configuración Básica] se encarga de implantar las barreras de defensa, preferiblemente para un entorno casero. Después, la opción [Configuración Avanzada] sirve para incluir un mayor número de ajustes, ideados para una red con un tránsito considerable de información entre varios PCs. Si éste no es tu caso, marca la primera posibilidad antes de pulsar el botón [Próximo >].

5 Como suele ocurrir habitualmente, el firewall que utiliza FortiClient dirige su barrera hacia la dirección IP del servidor predeterminado. Así lo puedes comprobar en la pantalla

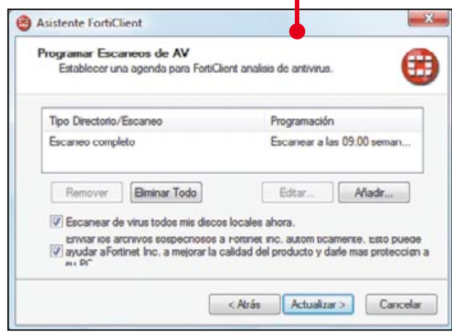
aunque, por supuesto, siempre es posible incluir la descripción de un servidor adicional pulsando el botón [Añadir...], y utilizando el formulario que aparece en pantalla posteriormente.

6 Otra posibilidad que también puedes definir a través del asistente de FortiClient es la que tiene relación con los servidores proxy. De esta forma, a través de la pantalla emergente



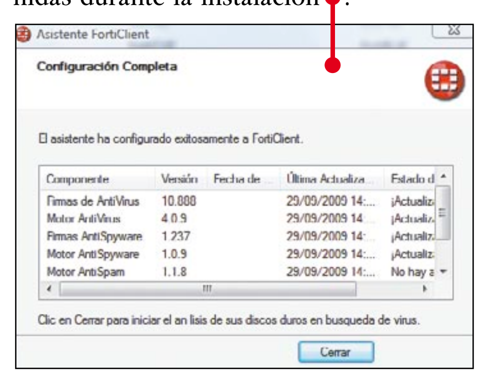
es posible introducir manualmente las características de este tipo de dispositivos, tras marcar previamente la casilla [Habilitar proxy para envío de virus].

7 Luego, para poder despreocuparte de las revisiones periódicas en busca de virus residentes en memoria, la aplicación permite, asimismo, programar sus escaneos mediante la pantalla.



Ten en cuenta que, por defecto, se incluye una revisión de los sistemas a primera hora de la mañana, aunque siempre se puede eliminar esta preferencia o añadir cualquier otra franja que consideres más oportuna. También es recomendable que actives la casilla verificable [Escanear de virus todos mis discos locales ahora.] para que, tras finalizar el asistente, se revise la fiabilidad de los contenidos almacenados en memoria. Asimismo, la casilla [Enviar los archivos sospechosos a Fortinet Inc. automáticamente. Esto puede ayudar a Fortinet Inc. a mejorar la calidad del producto y darle mas protección a su PC] hace posible el envío de muestras de virus detectados para diseñar, en el menor tiempo posible, la vacuna más eficaz. A continuación, para salir de este apartado presiona el botón [Actualizar >].

8 Como resultado de su configuración previa, una última pantalla muestra un resumen de todas las características definidas durante la instalación.



Para dar por concluido este primer proceso, haz click sobre la entrada Cerrar.

9 Antes de poder acceder a su interfaz principal, y debido a que así quedó registrado en un paso anterior del asistente, FortiClient realiza un análisis general para detectar y neutralizar malware en el equipo. El desarrollo de esta revisión queda reflejado mediante la ventana emergente.



10 Una que vez completado el primer chequeo de la memoria del ordenador, FortiClient incluye su icono dentro de la barra inferior de Windows.

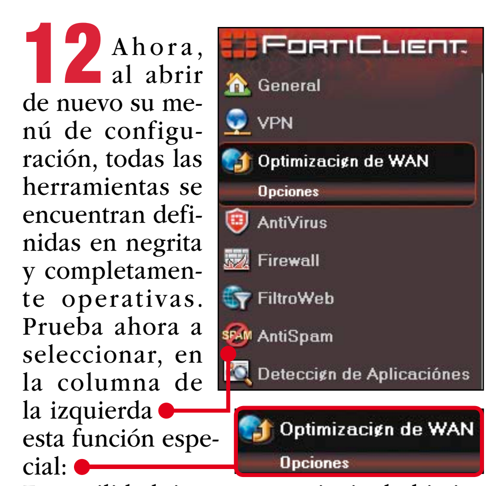
Para activar su interfaz principal, haz ahora doble click sobre su símbolo.



Como en este momento puedes contemplar, su presentación es muy sencilla: mientras que a la izquierda se listan en una columna sus aplicaciones, a la derecha se presenta una ventana explicativa para cada apartado.

11 Sin embargo, lo más probable es que no puedas acceder a muchas de sus opciones de uso, todavía deshabilitadas y presentadas en pantalla con una fuente en gris. Esto se debe a que el programa no se ejecuta por defecto en la modalidad de usuario administrador. Para conseguir activar todas las funciones que te ofrece este entorno, busca en la pantalla correspondiente al apartado General: Estado el botón Ejecutar cono administrador, y después haz click sobre él.

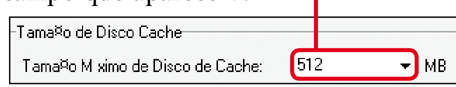
12 Ahora, al abrir de nuevo su menú de configuración, todas las herramientas se encuentran definidas en negrita y completamente operativas. Prueba ahora a seleccionar, en la columna de la izquierda esta función especial:



Esta utilidad tiene como principal objetivo optimizar las conexiones de red WAN, a partir de la modificación automática de parámetros técnicos, como son la capacidad del ancho de banda, la latencia o el control de paquetes de información.



No obstante, la herramienta tan sólo requiere verificar las áreas de mejora que se desee, marcando sus correspondientes casillas en blanco, para luego definir la cantidad de la memoria caché dentro del campo que aparece.

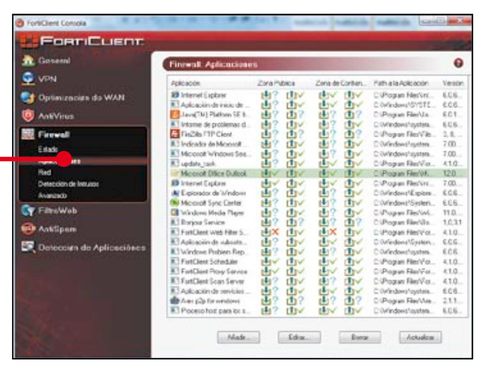


Para poner este recurso en funcionamiento, pulsa el botón Aplicar.

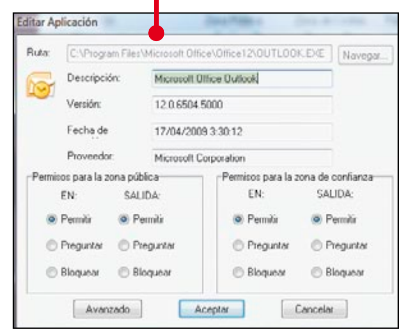
13 Otra de las ventajas que aporta FortiClient es la discriminación que realiza su firewall para cada una de las aplicaciones activas. Para revisar esta opción, selecciona la entrada especial Firewall y, a continuación, escoge dentro de su menú la variante.



Como resultado de esta operación, una nueva pantalla lista todos los programas que están siendo ejecutados en ese mismo momento, con los atributos asignados para sus transferencias de datos en zonas online públicas o de confianza.

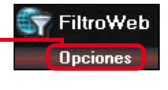


14 Llegados a este punto, selecciona en el listado, con la ayuda del cursor, la línea del programa que te interese definir, y después haz click sobre el comando Editar... Ahora, dentro de la ventana emergente que te aparezca, ya es posible establecer los parámetros que consideres más adecuados.



Concretamente, presta atención a las secciones denominadas Permisos para la zona pública y Permisos para la zona de confianza. Para cada una de ellas se incluyen, además, dos columnas: una de entrada de datos y otra de salida, que poseen tres posibles medidas. Así, con Permitir el programa deja paso libre al traslado de datos, con Preguntar requiere antes una verificación previa y, con la opción Bloquear, se anula al instante la comunicación entre la utilidad y el servidor habilitado. Ten por seguro que, si te tomas algo de tiempo para ajustar los parámetros de todas las aplicaciones aquí detalladas, el firewall de FortiClient se encargará de frenar cualquier intento de intrusismo, al mismo tiempo que optimiza el resto de enlaces permitidos.

15 Por último, si acudes al apartado



y te diriges a su menú de configuración



al hacer click sobre el control denominado Modificar Opciones se abre automáticamente un amplio menú para que puedas configurar el filtro web



una herramienta esencial para restringir el acceso a ciertos contenidos de Internet.